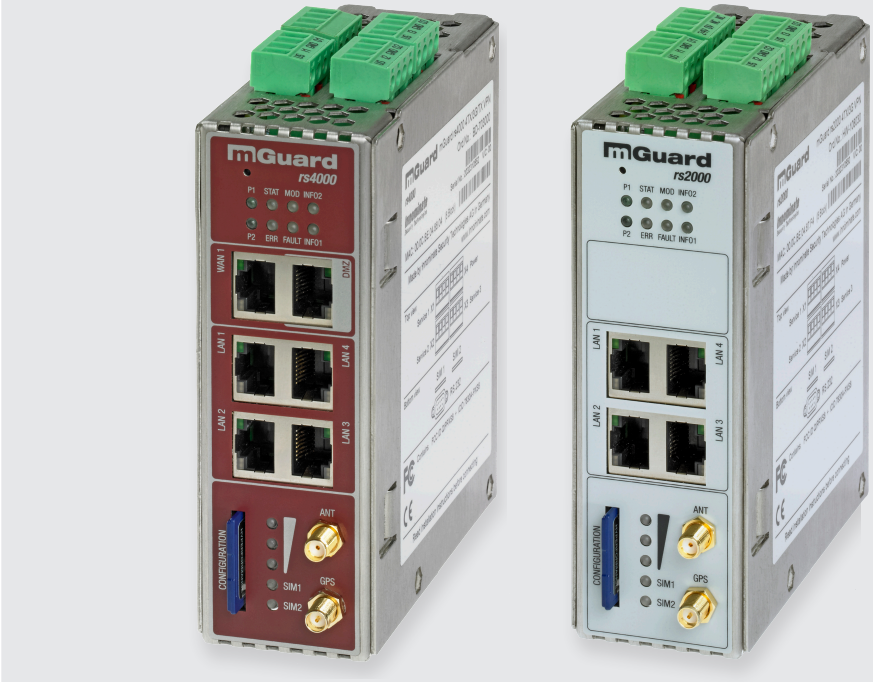
mGuard
Firmware 8.1

Configuration of the mGuard Security Appliances

Software Reference Manual



Innominate
Security Technologies

Software Reference Manual
mGuard Firmware 8.1

2015-01-27

Designation: UM EN MGUARD 8.1

Revision: 02

Order No.: —

This user manual is valid for the mGuard software release 8.1 when using devices of the mGuard product range:

- mGuard rs4000 3G
- mGuard rs2000 3G
- mGuard rs4000
- mGuard rs2000
- mGuard centerport
- mGuard industrial rs
- mGuard smart²
- mGuard smart
- mGuard pci² SD
- mGuard pcie² SD
- mGuard blade
- mGuard delta²
- mGuard delta
- EAGLE mGuard

Please observe the following notes

Target group of this user manual

The use of products described in this user manual is aimed solely at:

– Qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.
– Qualified application programmers and software engineers, who are familiar with the safety concepts of automation technology as well as applicable standards and other regulations.

Explanation of symbols used and signal words

This symbol indicates hazards that could lead to personal injury. Obey all safety measures that follow this symbol to avoid possible injury or death.

There are three different categories of personal injury that are indicated by a signal word.

DANGER This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

This symbol together with the signal word **NOTE** and the accompanying text alert the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.

This symbol and the accompanying text provide the reader with additional information or refer to detailed sources of information.

General terms and conditions of use for technical documentation

Innominate reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Innominate to furnish information on modifications to products and/or technical documentation. You are responsible for verifying the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Innominate apply exclusively, in particular as concerns any warranty liability.

This user manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document are prohibited.

Innominate reserves the right to register its own intellectual property rights for the product identifications of Innominate products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

“Innominate” and “mGuard” are registered trade names of Innominate Security Technologies AG. mGuard technology is protected by patents 10138865 and 10305413, granted by the German Patent and Trademark Office, and by US patents 7,430,759 and 8,146,144. Further patents are pending.

Published by

Innominate Security Technologies AG

Rudower Chaussee 13
12489 Berlin
Germany
Phone: +49 (0)30 92 10 28-0
contact@innominate.com

www.innominate.com

© 27. January 2015 Innominate Security Technologies AG

Innominate document number: UG208102814-053

Table of contents

1 mGuard basics 11

1.1 Basic properties of the mGuards 11

1.2 Typical application scenarios 13

1.2.1 Stealth mode (Plug-n-Protect) 13

1.2.2 Network router 14

1.2.3 DMZ 15

1.2.4 VPN gateway 15

1.2.5 WLAN via VPN 16

1.2.6 Resolving network conflicts 17

2 Configuration help 19

2.1 Suitable browsers 19

2.2 User roles 19

2.3 Input help during configuration (system messages) 20

2.4 Using the web interface 21

2.5 CIDR (Classless Inter-Domain Routing) 24

2.6 Network example diagram 25

3 Changes compared to the previous version 27

3.1 Overview of modifications in version 8.1 27

3.1.1 User firewall in VPN connections 27

3.1.2 Dynamic activation of the firewall rules (conditional firewall) 27

3.1.3 Function extension of the service contacts 28

3.1.4 OPC Inspector for Deep Packet Inspection for OPC Classic 29

3.1.5 Additional functions 29

3.2 Overview of modifications in version 8.0 30

3.2.1 New in CIFS Integrity Monitoring 31

3.2.2 VPN extensions 31

4 Management menu 33

4.1 Management >> System Settings 33

4.1.1 Host 33

4.1.2 Time and Date 35

4.1.3 Shell Access 40

4.1.4 E-Mail 52

4.2 Management >> Web Settings 56

4.2.1 General 56

4.2.2 Access 57

4.3 Management >> Licensing 67

4.3.1 Overview 67

4.3.2 Install 67

4.3.3 Terms of License 69

4.3.4 Management >> Update 70

4.3.5 Overview 70

4.3.6 Update 71

4.4 Management >> Configuration Profiles 74
4.4.1 Configuration Profiles 74
4.5 Management >> SNMP 79
4.5.1 Query 79
4.5.2 Trap 83
4.5.3 LLDP 90
4.6 Management >> Central Management 91
4.6.1 Configuration Pull 91
4.7 Management >> Service I/O 95
4.7.1 Service I/O 96
4.7.2 Alarm output 98
4.8 Management >> Restart 100
4.8.1 Restart 100

5 Blade Control menu 101
5.1 Blade Control >> Overview 101
5.2 Blade Control >> Blade 01 to 12 102
5.2.1 Blade in slot #... 102
5.2.2 Configuration 103

6 Network menu 105
6.1 Network >> Interfaces 105
6.1.1 General 106
6.1.2 Dial-out 130
6.1.3 Dial-in 136
6.1.4 Modem/Console 139
6.2 Network >> Ethernet 148
6.2.1 MAU settings 148
6.2.2 Multicast 150
6.2.3 Ethernet 151
6.3 Network >> NAT 152
6.3.1 Masquerading 152
6.3.2 IP and Port Forwarding 155
6.4 Network >> DNS 157
6.4.1 DNS server 157
6.4.2 DynDNS 160
6.5 Network >> DHCP 162
6.5.1 Internal/External DHCP 162
6.6 Network >> Proxy Settings 167
6.6.1 HTTP(S) Proxy Settings 167
6.7 Network >> Mobile Network 168
6.7.1 General 169
6.7.2 SIM Settings 174
6.7.3 Text message Notifications 177
6.7.4 Positioning system 179

7 Authentication menu 181
7.1 Authentication >> Administrative Users 181
7.1.1 Passwords 181
7.1.2 RADIUS Filters 183
7.2 Authentication >> Firewall Users 185
7.2.1 Firewall Users 185
7.2.2 Access 186
7.2.3 Status 187
7.3 Authentication >> RADIUS 187
7.4 Authentication >> Certificates 190
7.4.1 Certificate settings 195
7.4.2 Machine Certificates 197
7.4.3 CA Certificates 199
7.4.4 Remote Certificates 201
7.4.5 CRL 203
8 Network Security menu 205
8.1 Network Security >> Packet Filter 205
8.1.1 Incoming rules 206
8.1.2 Outgoing rules 208
8.1.3 DMZ 210
8.1.4 Rule Records 212
8.1.5 MAC Filtering 215
8.1.6 Advanced 216
8.1.7 Firewall for the mGuard rs2000 (3G) 222
8.2 Network Security >> DoS Protection 223
8.2.1 Flood Protection 223
8.3 Network Security >> User Firewall 225
8.3.1 User Firewall Templates 225
9 CIFS Integrity Monitoring menu 229
9.1 CIFS Integrity Monitoring >> Importable Shares 230
9.1.1 Importable Shares 230
9.2 CIFS Integrity Monitoring >> CIFS Integrity Checking 232
9.2.1 Settings 233
9.2.2 Filename Patterns 240
9.3 CIFS Integrity Monitoring >> CIFS AV Scan Connector 242
9.3.1 CIFS Antivirus Scan Connector 242

10 IPsec VPN menu 247
10.1 IPsec VPN >> Global 247
10.1.1 Options 247
10.1.2 DynDNS Monitoring 253
10.2 IPsec VPN >> Connections 254
10.2.1 Connections 255
10.2.2 General 257
10.2.3 Authentication 269
10.2.4 Firewall 276
10.2.5 IKE Options 279
10.3 IPsec VPN >> L2TP over IPsec 284
10.3.1 L2TP Server 284
10.4 IPsec VPN >> IPsec Status 285
11 SEC-Stick menu 287
11.1 Global 288
11.2 Connections 291
12 QoS menu 293
12.1 Ingress Filters 293
12.1.1 Internal/External 293
12.2 Egress Queues 296
12.2.1 Internal/External/External 2/Dial-in 296
12.3 Egress Queues (VPN) 298
12.3.1 VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in 298
12.4 Egress Rules 301
12.4.1 Internal/External/External 2/Dial-in 301
12.4.2 Egress Rules (VPN) 302
13 Redundancy menu 305
13.1 Redundancy >> Firewall Redundancy 305
13.1.1 Redundancy 305
13.1.2 Connectivity Checks 313
13.2 Redundancy >> FW Redundancy Status 315
13.2.1 Redundancy Status 315
13.2.2 Connectivity Status 318
13.3 Ring/Network Coupling 320
13.3.1 Ring/Network Coupling 320
14 Logging menu 321
14.1 Logging >> Settings 321
14.1.1 Settings 321
14.2 Logging >> Browse local logs 323
14.2.1 Log entry categories 324

15 Support menu 327
15.1 Support >> Tools 327
15.1.1 Ping Check 327
15.1.2 Traceroute 327
15.1.3 DNS Lookup 328
15.1.4 IKE Ping 328
15.2 Support >> Advanced 329
15.2.1 Hardware 329
15.2.2 Snapshot 329
16 Redundancy 331
16.1 Firewall redundancy 331
16.1.1 Components in firewall redundancy 332
16.1.2 Interaction of the firewall redundancy components 334
16.1.3 Firewall redundancy settings from previous versions 334
16.1.4 Requirements for firewall redundancy 334
16.1.5 Fail-over switching time 335
16.1.6 Error compensation through firewall redundancy 337
16.1.7 Handling firewall redundancy in extreme situations 338
16.1.8 Interaction with other devices 340
16.1.9 Transmission capacity with firewall redundancy 343
16.1.10 Limits of firewall redundancy 344
16.2 VPN redundancy 345
16.2.1 Components in VPN redundancy 345
16.2.2 Interaction of the VPN redundancy components 346
16.2.3 Error compensation through VPN redundancy 346
16.2.4 Setting the variables for VPN redundancy 347
16.2.5 Requirements for VPN redundancy 348
16.2.6 Handling VPN redundancy in extreme situations 348
16.2.7 Interaction with other devices 350
16.2.8 Transmission capacity with VPN redundancy 352
16.2.9 Limits of VPN redundancy 353
17 Glossary 357

1 mGuard basics

The mGuard protects IP data links by combining the following functions:

– VPN router (VPN - **V**irtual **P**rivate **N**etwork) for secure data transmission via public networks (hardware-based DES, 3DES, and AES encryption, IPsec protocol).
– Configurable firewall for protection against unauthorized access. The dynamic packet filter inspects data packets using the source and destination address and blocks undesired data traffic.
– Network card (mGuard pci² SD, mGuard pcie² SD, mGuard pci), switch (mGuard delta, mGuard rs4000/rs2000 3G), 3G mobile phone and dedicated DMZ port (mGuard rs4000 3G)

1.1 Basic properties of the mGuards

Network features

– Stealth (auto, static, multi), router (static, DHCP client), PPPoE (for DSL), PPTP (for DSL), and modem
– VLAN
– DHCP server/relay on the internal and external network interfaces
– DNS cache on the internal network interface
– Administration via HTTPS and SSH
– Optional conversion of DSCP/TOS values (Quality of Service)
– Quality of Service (QoS)
– LLDP
– MAU management
– SNMP

Firewall features

– Stateful packet inspection
– Anti-spoofing
– IP filter
– L2 filter (only in stealth mode)
– NAT with FTP, IRC, and PPTP support (only in router modes)
– 1:1 NAT (only in *router* network mode)
– Port forwarding (not in *stealth* network mode)
– Individual firewall rules for different users (user firewall)
– Individual rule sets as action (target) of firewall rules (apart from user firewall or VPN firewall)

Anti-virus features

– CIFS integrity check of network drives for changes to specific file types (e.g., executable files)
– Anti-virus scan connector which supports central monitoring of network drives with virus scanners

VPN features

- Protocol: IPsec (tunnel and transport mode)
- IPsec encryption in hardware with DES (56 bits), 3DES (168 bits), and AES (128, 192, 256 bits)
- Packet authentication: MD5, SHA-1
- Internet Key Exchange (IKE) with main and quick mode
- Authentication via:
  - Pre-shared key (PSK)
  - X.509v3 certificates with public key infrastructure (PKI) with certification authority (CA), optional certificate revocation list (CRL), and the option of filtering by subject

  or
  - Partner certificate, e.g., self-signed certificates
- Detection of changing partner IP addresses via DynDNS
- NAT traversal (NAT-T)
- Dead Peer Detection (DPD): detection of IPsec connection aborts
- IPsec/L2TP server: connection of IPsec/L2TP clients
- IPsec firewall and 1:1 NAT
- Default route over VPN tunnel
- Data forwarding between VPNs (hub and spoke)
- Depending on the license: up to 250 VPN channels, in the case of mGuard centerport up to 1000 active VPN channels
- Hardware acceleration for encryption in the VPN tunnel (except for mGuard centerport)

Additional features

- Remote Logging
- Router/firewall redundancy (depending on the license)
- Administration using SNMP v1 - v3 and Innominate Device Manager (mGuard device manager)
- PKI support for HTTPS/SSH remote access
- Can act as an NTP and DNS server via the LAN interface
- Compatible with MGUARD Secure Cloud
- Plug-n-Protect technology
- Tracking and time synchronization via GPS/GLONASS positioning system

Support

In the event of problems with your mGuard, please contact your dealer.

Additional information on the device as well as on release notes and software updates can be found on the Internet at: www.innominate.com.

1.2 Typical application scenarios

This section describes various application scenarios for the mGuard.

- Stealth mode (Plug-n-Protect)
- Network router
- DMZ (Demilitarized Zone)
- VPN gateway
- WLAN via VPN tunnel
- Resolving network conflicts
- Mobile phone router via integrated mobile phone modem

1.2.1 Stealth mode (Plug-n-Protect)

In **stealth mode**, the mGuard can be positioned between an individual computer and the rest of the network.

The settings (e.g., for firewall and VPN) can be made using a web browser under the URL https://1.1.1.1/.

No configuration modifications are required on the computer itself.

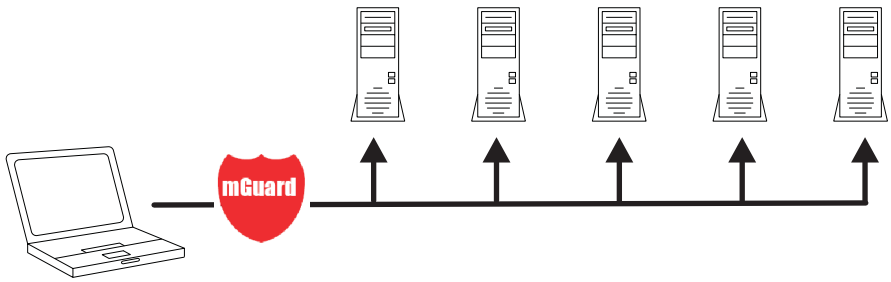


Figure 1-1 Stealth mode (Plug-n-Protect)

1.2.2 Network router

When used as a **network router**, the mGuard can provide the Internet link for several computers and protect the company network with its firewall.

One of the following network modes can be used on the mGuard:

– *Router*, if the Internet connection is, for example, via a DSL router or a permanent line.
– *PPPoE*, if the Internet connection is, for example, via a DSL modem and the PPPoE protocol is used (e.g., in Germany).
– *PPTP*, if the Internet connection is, for example, via a DSL modem and the PPTP protocol is used (e.g., in Austria).
– *Modem*, if the Internet connection is via a serial connected modem (compatible with Hayes or AT command set).
– *Built-in mobile phone modem*, mobile phone router via integrated mobile phone modem

For computers in the Intranet, the mGuard must be specified as the default gateway.

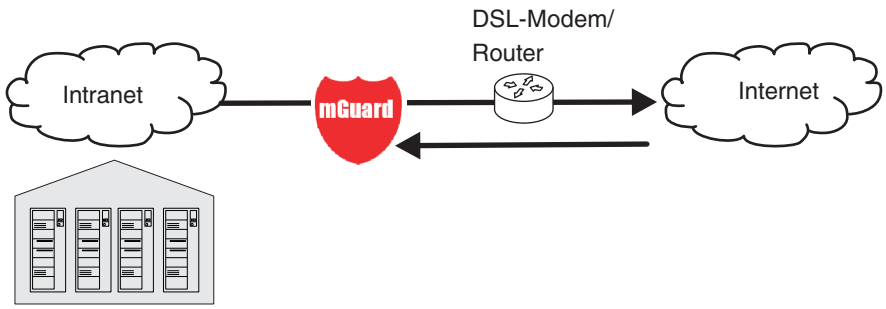


Figure 1-2 Network router

1.2.3 DMZ

A **DMZ** (demilitarized zone) is a protected network that is located between two other networks. For example, a company's website may be in the DMZ so that new pages can only be copied to the server from the Intranet using FTP. However, the pages can be read from the Internet via HTTP.

IP addresses within the DMZ can be public or private, and the mGuard, which is connected to the Internet, forwards the connections to private addresses within the DMZ by means of port forwarding.

A DMZ scenario can be established either between two mGuards (see Figure 1-3), or via a dedicated DMZ port of the mGuard rs4000 3G.

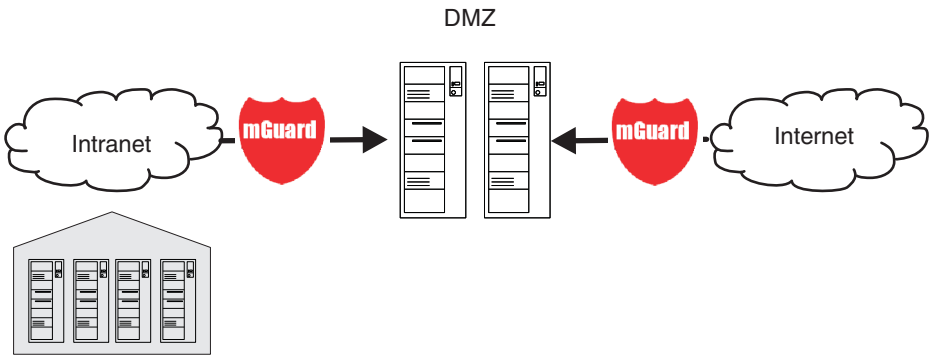


Figure 1-3 DMZ

1.2.4 VPN gateway

The **VPN gateway** provides company employees with encrypted access to the company network from home or when traveling. mGuard performs the role of the VPN gateway.

IPsec-capable VPN client software must be installed on the external computers or failing that, the computer is equipped with a mGuard.

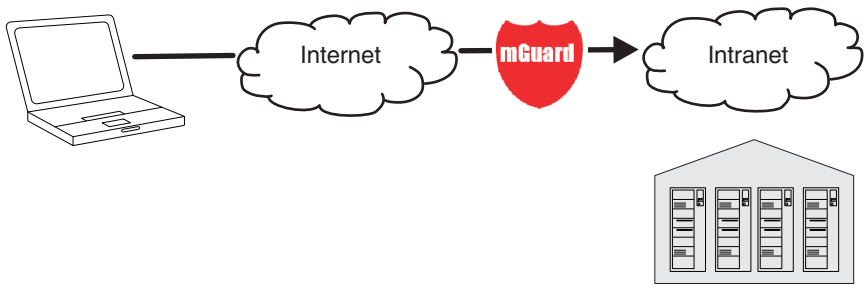


Figure 1-4 VPN gateway

1.2.5 WLAN via VPN

WLAN via VPN is used to connect two company buildings via a WLAN path protected using IPsec. The annex should also be able to use the Internet connection of the main building.

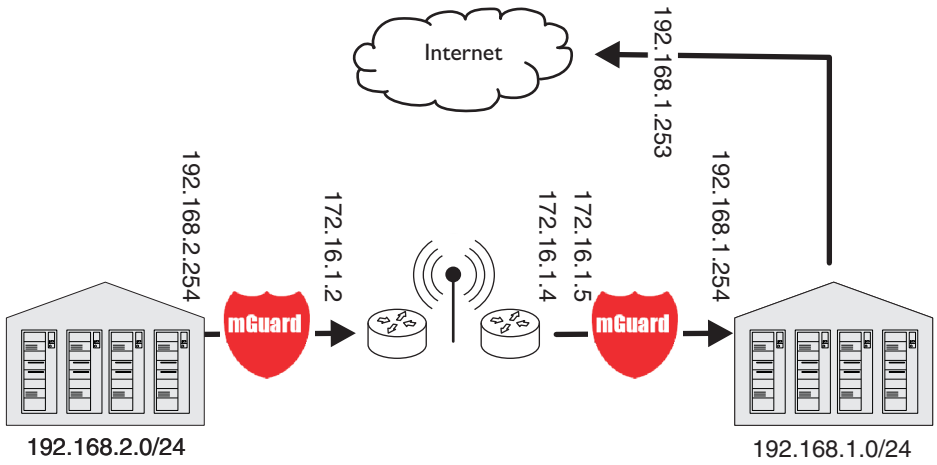


Figure 1-5 WLAN via VPN

In this example, the mGuard devices were set to *router* mode and a separate network with 172.16.1.x addresses was set up for the WLAN.

To provide the annex with an Internet connection via the VPN, a default route is set up via the VPN:

Tunnel configuration in the annex

Connection type	Tunnel (network <-> network)
Address of the local network	192.168.2.0/24
Address of the remote network	0.0.0.0/0

In the main building, the corresponding counterpart is configured:

Tunnel configuration in the main building

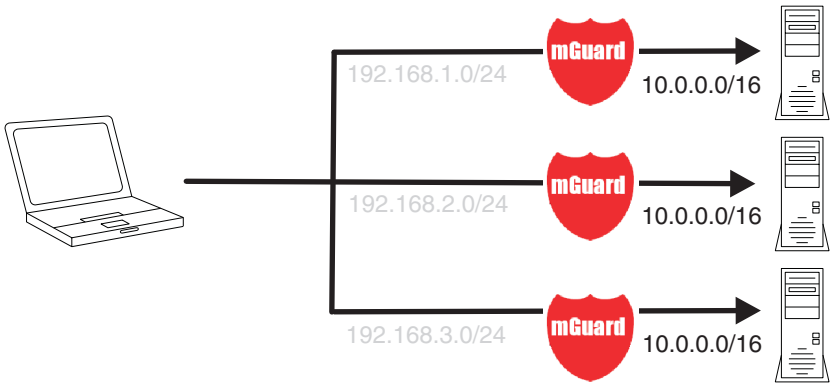
Connection type	Tunnel (network <-> network)
Local network	0.0.0.0
Address of the remote network	192.168.2.0/24

The default route of an mGuard usually uses the WAN port. However, in this case the Internet can be accessed via the LAN port:

Default gateway in the main building:

IP address of default gateway	192.168.1.253

1.2.6 Resolving network conflicts



Resolving network conflicts

In the example, the networks on the right-hand side should be accessible to the network or computer on the left-hand side. However, for historical or technical reasons the networks on the right-hand side overlap.

The 1:1 NAT feature of the mGuard can be used to translate these networks to other networks, thereby resolving the conflict.

(1:1 NAT can be used in normal routing and in IPsec tunnels.)

2 Configuration help

2.1 Suitable browsers

The device can be configured easily using a web browser.

To configure the mGuard, use a web browser with SSL encryption (HTTPS).

Browsers with SSL encryption (HTTPS) approved by Innominate:

– Mozilla **Firefox,** Version 4 or later
– Google **Chrome,** Version 12 or later
– Microsoft **Internet Explorer**, Version 8 or later
– Apple **Safari**, Version 5.1.7 or later

Further information can be found on the Innominate website at: www.innominate.com .

Limitation of login attempts

In the event of a Denail of Service attack, services are intentionally made unable to function. To prevent this type of attack, the mGuard is provided with a choke for different network requests.

This feature is used to count all connections going out from one IP address and using a specific protocol. When counting a specific number of connections without a valid login, the choke becomes effective. If no invalid connection attempt is made for the duration of 30 seconds, the choke is reset. Each new request without valid login from this IP address resets the timer by 30 seconds.

The number of connection attempts that need to fail until the choke becomes effective depends on the protocol.

– 20 when using HTTPS
– 6 when using SSH, SNMP, COM server

2.2 User roles

root	User role without restrictions
admin	Administrator
netadmin	Administrator for the network only
audit	Auditor/tester

The predefined users (*root*, *admin*, *netadmin*, and *audit*) have different permissions.

– The *root* user has unrestricted access to the mGuard.
– The *admin* user also has unrestricted functional access to the mGuard, however the number of simultaneous SSH sessions is limited.
– Permissions are explicitly assigned to the *netadmin* user via the mGuard device manager. This user only has read access to the other functions. Passwords and private keys cannot be read by this user.
– This *audit* user only has read access to all functions. By default, the *audit* user role can only be activated via the mGuard device manager, in the same way as *netadmin*.

2.3 Input help during configuration (system messages)

With firmware 8.0 or later, modified or invalid entries are highlighted in color on the web interface.

With firmware 8.1 or later, dynamic values are displayed in red. In this way, status messaged indicating a current value can be recognized more easily.

System messages which explain why an entry is invalid, for example, are also displayed.

The browser used must allow JavaScript for this support to function.

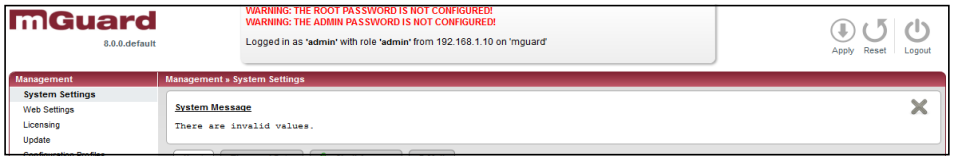


Figure 2-1 Example system message

- **Modified entries** are highlighted in **blue** on the relevant page and in the associated menu item until the changes are saved or reset. (Exception: modified tables)
- **Invalid entries** are highlighted in **red** on the relevant page and tab and in the associated menu item.

The modified or invalid entries remain highlighted even when you close a menu.

When necessary, information relating to the system is displayed at the top of the screen. You can also open this area by clicking the letter icon.

2.4 Using the web interface

You can click on the desired configuration via the menu on the left-hand side, e.g., “Management, Licensing”.

The page is then displayed in the main window – usually in the form of one or more tab pages – where settings can be made. If the page is organized into several tab pages, you can switch between them using the *tabs* at the top.

Working with tab pages

– You can make the desired entries on the corresponding tab page (see also “Working with sortable tables” on page 22).

– You can return to the previously accessed page by clicking on the **Back** button located at the bottom right of the page, if available.

Entry of impermissible values

If you enter an impermissible value (e.g., an impermissible number in an IP address) and click on the **Apply** button, the relevant tab page title is displayed in red. This makes it easier to trace the error.

Buttons

The following buttons are located at the top of every page:

Logout

For logging out after configuration access to the mGuard.

If the user does not log out, he/she is logged out automatically if there has been no further activity and the time period specified by the configuration has elapsed. Access can only be restored by logging in again.

Reset

Resets to the original values. If you have entered values on a configuration page and these have not yet taken effect (by clicking on the **Apply** button), you can restore the original values on the page by clicking the **Reset** button.

Apply

To apply the settings on the device, you must click on the **Apply** button. This applies across all pages.

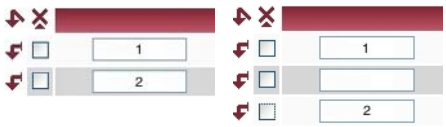
Working with sortable tables

Many settings are saved as data records. Accordingly, the adjustable parameters and their values are presented in the form of table rows. If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. Therefore, note the order of the entries, if necessary. The order can be changed by moving table rows up or down.

With tables you can:

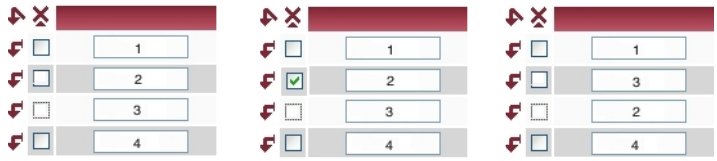
– Insert rows to create a new data record with settings (e.g., the firewall settings for a specific connection)
– Move rows (i.e., resort them)
– Delete rows to delete the entire data record

Inserting rows



1. Click on the arrow below which you want to insert a new row.
2. The new row is inserted.
   You can now enter or specify values in the row.

Moving rows



1. Select the row(s) you want to move.
2. Click on the arrow below which you want to move the selected rows.
3. The rows are moved.

Deleting rows

1. Select the rows you want to delete.
2. Click on to delete the rows.
3. The rows are deleted.

Working with non-sortable tables

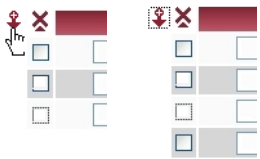
Tables are non-sortable if the order of the data records contained within them does not play any technical role. It is then not possible to insert or move rows. With these tables you can:

– Delete rows
– Append rows to the end of the table in order to create a new data record with settings (e.g., user firewall templates)

The symbols for inserting a new table row are therefore different:

– to append rows to a **non**-sortable table
– to insert rows in a sortable table

Appending rows (non-sortable tables)



1. Click on the arrow to append a new row.
2. The new row is appended below the existing table.
   You can now enter or specify values in the row.

2.5 CIDR (Classless Inter-Domain Routing)

IP subnet masks and CIDR are methods of notation that combine several IP addresses to create a single address area. An area comprising consecutive addresses is handled like a network.

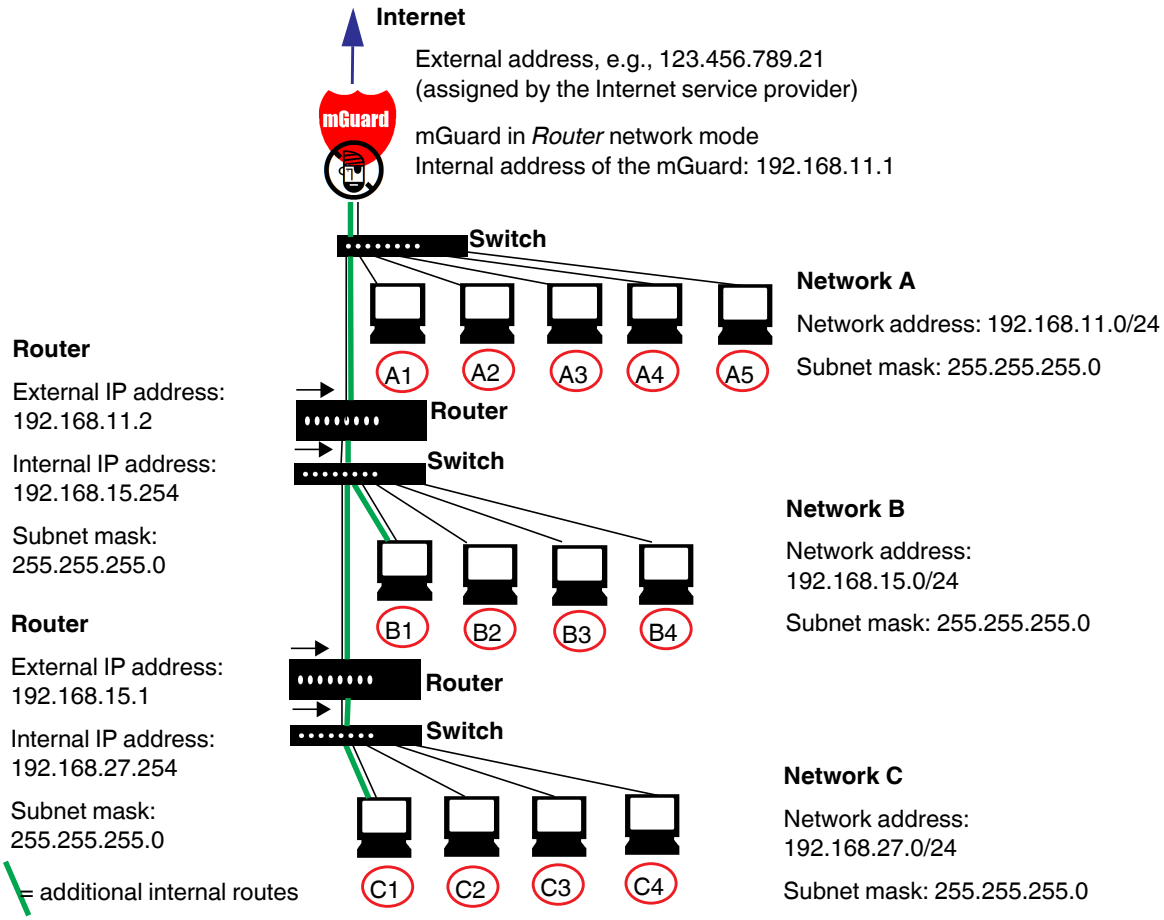
To specify an area of IP addresses for the mGuard, e.g., when configuring the firewall, it may be necessary to specify the address area in CIDR format. In the table below, the left-hand column shows the IP subnet mask, while the far right-hand column shows the corresponding CIDR notation.

IP subnet mask	Binary	CIDR
255.255.255.255	11111111 11111111 11111111 11111111	32
255.255.255.254	11111111 11111111 11111111 11111110	31
255.255.255.252	11111111 11111111 11111111 11111100	30
255.255.255.248	11111111 11111111 11111111 11111000	29
255.255.255.240	11111111 11111111 11111111 11110000	28
255.255.255.224	11111111 11111111 11111111 11100000	27
255.255.255.192	11111111 11111111 11111111 11000000	26
255.255.255.128	11111111 11111111 11111111 10000000	25
255.255.255.0	11111111 11111111 11111111 00000000	24
255.255.254.0	11111111 11111111 11111110 00000000	23
255.255.252.0	11111111 11111111 11111100 00000000	22
255.255.248.0	11111111 11111111 11111000 00000000	21
255.255.240.0	11111111 11111111 11110000 00000000	20
255.255.224.0	11111111 11111111 11100000 00000000	19
255.255.192.0	11111111 11111111 11000000 00000000	18
255.255.128.0	11111111 11111111 10000000 00000000	17
255.255.0.0	11111111 11111111 00000000 00000000	16
255.254.0.0	11111111 11111110 00000000 00000000	15
255.252.0.0	11111111 11111100 00000000 00000000	14
255.248.0.0	11111111 11111000 00000000 00000000	13
255.240.0.0	11111111 11110000 00000000 00000000	12
255.224.0.0	11111111 11100000 00000000 00000000	11
255.192.0.0	11111111 11000000 00000000 00000000	10
255.128.0.0	11111111 10000000 00000000 00000000	9
255.0.0.0	11111111 00000000 00000000 00000000	8
254.0.0.0	11111110 00000000 00000000 00000000	7
252.0.0.0	11111100 00000000 00000000 00000000	6
248.0.0.0	11111000 00000000 00000000 00000000	5
240.0.0.0	11110000 00000000 00000000 00000000	4
224.0.0.0	11100000 00000000 00000000 00000000	3
192.0.0.0	11000000 00000000 00000000 00000000	2
128.0.0.0	10000000 00000000 00000000 00000000	1

Example: 192.168.1.0/255.255.255.0 corresponds to CIDR: 192.168.1.0/24

2.6 Network example diagram

The following diagram shows how IP addresses can be distributed in a local network with subnetworks, which network addresses result from this, and how the details regarding additional internal routes may look for the mGuard.



Network A	**Computer**	**A1**	**A2**	**A3**	**A4**	**A5**
	IP address	192.168.11.3	**192.168.11.4**	**192.168.11.5**	**192.168.11.6**	**192.168.11.7**
	Subnet mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**
Network B	**Computer**	**B1**	**B2**	**B3**	**B4**	
	IP address	192.168.15.2	**192.168.15.3**	**192.168.15.4**	**192.168.15.5**	
	Subnet mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	
Network C	**Computer**	**C1**	**C2**	**C3**	**C4**	
	IP address	192.168.27.1	**192.168.27.2**	**192.168.27.3**	**192.168.27.4**	
	Subnet mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	

Additional internal routes:
Network: 192.168.15.0/24
Gateway: 192.168.11.2
Network: 192.168.27.0/24
Gateway: 192.168.11.2

3 Changes compared to the previous version

3.1 Overview of modifications in version 8.1

The following functions have been added to firmware Version 8.1.

- User firewall in VPN connections
- Dynamic activation of the firewall rules
- Function extension of the service contacts
- OPC Inspector for Deep Packet Inspection for OPC Classic
- Extended DynDNS providers
- New mode for Pre-Shared Secret authentication method
- On the web interface, dynamic modifications are displayed in red.
- Detailed logging of modems

3.1.1 User firewall in VPN connections

The user firewall can be used within VPN connections.

A VPN connection in which the user firewall rules apply can now be selected for the user firewall (under Network Security >> User Firewall >> User Firewall Templates.

3.1.2 Dynamic activation of the firewall rules (conditional firewall)

The firewall rules can now be activated via an external event:

- **A button on the web interface** (under Network Security >> Packet Filter >> Rule Records)
- **An API command line** that is activated using the name or the row ID. /Packages/mguard-api_0/mbin/action fwrules/[in]active <ROWID>
- /Packages/mguard-api_0/mbin/action_name fwrules/[in]active <NAME>
- **An externally connected button/switch** (for mGuards that allow connection, see “Dynamic activation of the firewall rules (conditional firewall)” on page 27)
- **Establishing or releasing a VPN connection**. It can be set whether an established VPN connection activates or deactivates the firewall rule.
- **Incoming text message** (for mGuard rs4000/rs2000 3G only). See „Token for text message trigger“ under Network Security >> Packet Filter >> Rule Records.
- **CGI interface**. The “nph-action.cgi may” CGI script can be used to control firewall rules.

If the status of the firewall rule record changes, an e-mail can automatically be sent. With regard to the mGuard rs4000/rs2000 3G, a text message can also be sent in this case.

3.1.3 Function extension of the service contacts

Service contacts (service I/Os) can be connected to some mGuards.

- **mGuard rs4000/rs2000 3G**
- **mGuard rs4000/rs2000**
- **mGuard industrial rs**

A push button or an on/off switch can be connected to **inputs CMD 1-3**. The push button or on/off switch is used to establish and release predefined VPN connections or the defined firewall rule records.

For the VPN connections it can be set whether the VPN connection is to be switched via one of the service contacts (IPsec VPN >> Connections >> Edit >> General). If a switch is connected, the switch behavior can also be inverted.

For the firewall rule records it can be set whether a rule is to be switched via one of the service contacts or if a VPN connection is to be switched (Network Security >> Packet Filter >> Rule Records).

In this way, one or more freely selectable VPN connections or firewall rule records can be switched. A mixture of VPN connections and firewall rule records is also possible.

The web interface displays which VPN connections and which firewall rule records are connected to one input (Management >> Service I/O >> Service I/O).

In addition, the behavior of **outputs ACK 1-3** can be set on the web interface (Management >> Service I/O >> Service I/O).

Outputs ACK 1-2 can be used to monitor specific VPN connections or firewall rule records and to display them using LEDs.

Alarm output ACK 3 monitors the function of the mGuard and thus allows for error diagnostics.

The alarm output reports the following, if it has been activated.

- Failure of the redundant supply voltage
- Monitoring of the link status of the Ethernet connections
- Monitoring of the temperature condition
- Monitoring of the connection state of the internal modem

3.1.4 OPC Inspector for Deep Packet Inspection for OPC Classic

When using the OPC Classic network protocol, interconnected firewalls virtually have no effect. In addition, conventional NAT routing cannot be used.

When activating the OPC Classic function, the OPC packets are monitored (under Network Security >> Packet Filter >> Advanced).

The TCP ports that are negotiated during the connection opened first are detected and opened for OPC packets. If no OPC packets are transmitted via these ports within a configurable timeout, they are closed again. If the OPC validity check is activated, only OPC packets must be transmitted via OPC Classic port 135.

3.1.5 Additional functions

Extended DynDNS providers

– When establishing VPN connections, it is useful that the devices obtain their IP address via a DynDNS service.

  In version 8.1, more DynDNS providers are supported.

New mode for Pre-Shared Key authentication method

When selecting the Pre-Shared Key (PSK) authentication method, “Aggressive Mode” can be selected (under IPsec VPN >> Connections >> Edit >> Authentication).

On the web interface, dynamic modifications are highlighted red.

On the web interface, status messages are displayed and permanently updated. To recognize these entries more easily, they are displayed in red.

Detailed logging of modems

Only for mGuards that have an internal or external modem or that are capable of mobile communication (under Logging >> Settings).

3.2 Overview of modifications in version 8.0

The following functions have been added to firmware Version 8.0.

Configuration extensions

- Improved CIFS Integrity Monitoring (see “New in CIFS Integrity Monitoring” on page 31)
- Integrated **COM server** for mGuard platforms with serial interface (see “COM server for mGuard platforms with serial interface” on page 143)
- Configurable **multicast support** for devices with internal switch, in order to send data to a group of receivers without the transmitter having to send it multiple times (see “Multicast” on page 150)
- **VPN extensions** (see “VPN extensions” on page 31).
- **Dynamic web interface** for configuration. Incorrect entries are highlighted in color and help is also offered in the form of system messages (see “CIDR (Classless Inter-Domain Routing)” on page 24).

Support for mGuard platforms mGuard rs4000 3G and mGuard rs2000 3G

- Support for **mobile phone and positioning functions** (see “Network >> Mobile Network” on page 168)
- **Support for integrated managed and unmanaged Switches** (see “Network >> Ethernet” on page 148)
- Support for a dedicated **DMZ port** (only mGuard rs4000 3G)
  The DMZ port can be set so that it forwards packets to the internal, external or secondary external interface.
  The DMZ port is only supported in router mode and requires at least one IP address and a corresponding subnet mask. The DMZ does not support any VLANs.

Removed functions

- HiDiscovery support
- The “Accept” button which accepts changes for the current page only has been removed. Changes are made across all pages.

3.2.1 New in CIFS Integrity Monitoring

Time schedule

The time schedule has been improved in Version 8.0. Now more than one scan per day is possible. Continuous scanning can also be set.

If the scan takes longer than planned, it is aborted. However you can adjust the settings, so that a scan is started regularly.

Extended display of the current status

Each row of the CIFS Integrity Monitoring also indicates the following information.

– The status of the scanned importable shares
– The result of the last scan or the progress of the current scan

The menu in the web interface has been extended so that you can now see that status of each scan. The progress indicator shows the number of checked files.

3.2.2 VPN extensions

Status of the VPN extensions

The setting for the VPN connection is now divided into “Disabled”, “Started”, and “Stopped”. The “Disabled” setting ignores the VPN connection, as if this were not configured. This also means it cannot be dynamically enabled/disabled. The other two settings determine the status of the VPN connection when it is restarted or booted.

In Version 8.0, the VPN connections can be started or stopped via a button on the web interface, via text message, an external switch or the script nph-vpn.cgi. This takes into account all VPN connections. Packets that correspond to a VPN connection that is not disabled are forwarded when the connection is established or dropped if the connection is not established. VPN connections which were set to “Active: No” in the previous versions, are now interpreted as “Disabled”.

Unique names

In Version 8.0, the names of VPN connections are made unique. During the update, a hash or unique number is added to names that are duplicated.

Timeout for the VPN connection

You can set a timeout which aborts the VPN connection if it has been started via text message, nph-vpn.cgi or the web interface. VPN connections which have been started by an explicit request via an application are not affected.

Source-based routing

VPN tunnels which only differ in their source network can now be configured.

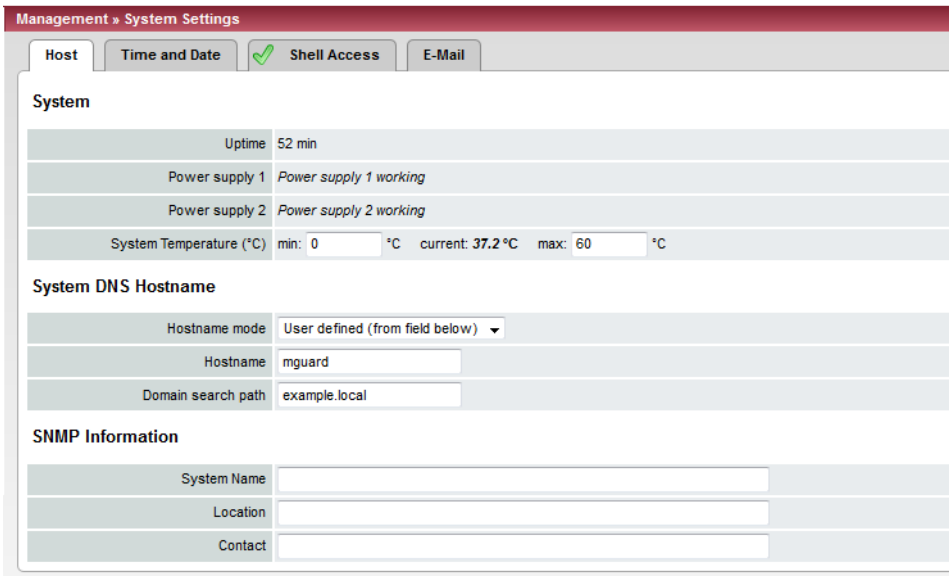
From Version 8.0, the VPN configuration permits a remote network with different local networks in one configuration. The VPN tunnel groups are extended so that they permit an established VPN connection to select only one subnetwork from the local network. In previous versions, this was only possible for remote networks.

4 Management menu

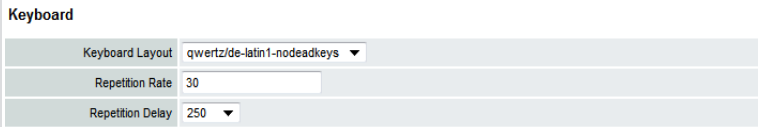
For security reasons, we recommend you change the default root and administrator passwords during initial configuration (see “Authentication >> Administrative Users” on page 181). A message informing you of this will continue to be displayed at the top of the page until the passwords are changed.

4.1 Management >> System Settings

4.1.1 Host

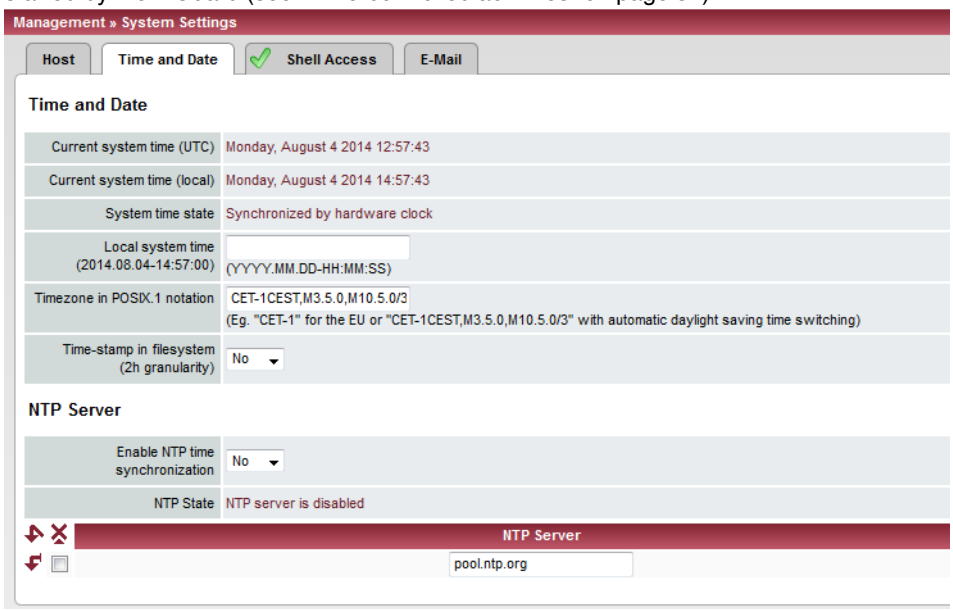


Management >> System Settings >> Host	
System	
	Uptime Device operating time since the last restart.
	(only mGuard rs4000 3G, mGuard rs4000, mGuard centerport, mGuard industrial rs, EAGLE mGuard)
	Power supply 1/2 State of both power supply units
	(only mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs, mGuard smart², mGuard pci² SD, mGuard pcie² SD, mGuard delta², EAGLE mGuard)
	System Temperature (°C) An SNMP trap is triggered if the temperature exceeds or falls below the specified temperature range.
	(only mGuard centerport, not with firmware 7.6.0)
	CPU temperature (°C) An SNMP trap is triggered if the temperature exceeds or falls below the specified temperature range.

Management >> System Settings >> Host [...]		
System DNS Hostname	**Hostname mode**	You can assign a name to the mGuard using the *Hostname mode* and *Hostname* fields. This name is then displayed, for example, when logging in via SSH (see “Management >> System Settings” on page 33, “Shell Access” on page 40). Assigning names simplifies the administration of multiple mGuard devices. **User defined (from field below)** (Default) The name entered in the “Hostname” field is the name used for the mGuard. If the mGuard is running in *Stealth* mode, the “User defined” option must be selected under “Hostname mode”. **Provider defined (e.g., via DHCP)** If the selected network mode permits external setting of the host name, e.g., via DHCP, the name supplied by the provider is assigned to the mGuard.
	Host name	If the “User defined” option is selected under “Hostname mode”, enter the name that should be assigned to the mGuard here. Otherwise, this entry will be ignored (i.e., if the “Provider defined” option (e.g., via DHCP) is selected under “Hostname mode”).
	Domain search path	This option makes it easier for the user to enter a domain name. If the user enters the domain name in an abbreviated form, the mGuard completes the entry by appending the domain suffix that is defined here under “Domain search path”.
SNMP Information	**System name**	A name that can be freely assigned to the mGuard for administration purposes, e.g., “Hermes”, “Pluto”. (Under SNMP: sysName)
	Location	A description of the installation location that can be freely assigned, e.g., “Hall IV, Corridor 3”, “Control cabinet”. (Under SNMP: sysLocation)
	Contact	The name of the contact person responsible for the mGuard, ideally including the phone number. (Under SNMP: sysContact)
Keyboard	**(only mGuard centerport)** 	
	Keyboard Layout	Selection list for selecting the appropriate keyboard layout.
	Repetition Rate	Determines how many characters the keyboard generates per second when a key is held down. (Default: 30)
	Repetition Delay	Determines how long a key must be held down on the keyboard until the repeat function takes effect and the number of characters defined above under **Repetition Rate** are generated per second. (Default: 250)

4.1.2 Time and Date

Set the time and date correctly. Otherwise, certain time-dependent activities cannot be started by the mGuard (see “Time-controlled activities” on page 37).



Management >> System Settings >> Time and Date		
Time and Date	**Current system time (UTC)**	The current system time is displayed as Universal Time Coordinates (UTCs). If **Enable NTP time synchronization** is not yet activated (see below) and **Time-stamp in filesystem** is deactivated, the clock will start at January 1, 2000.
	Current system time (local)	Display: If the (sometimes different) current local time should be displayed, the corresponding entry must be made under **Timezone in POSIX.1 notation** (see below).

Management >> System Settings >> Time and Date[...]		
	System time state	Indicates whether the mGuard system time has ever been synchronized with a currently valid time during mGuard runtime. **If the display indicates that the mGuard system time has not been synchronized, the mGuard does not perform any time-controlled activities**. Devices without built-in clock always start in “Not synchronized” mode. Devices with integrated clock usually start in “Synchronized by hardware clock” mode. The state of the clock only returns to “Not synchronized” if the firmware is reinstalled on the device or if the built-in clock has been disconnected from the power for too long. Power supply of the integrated clock is ensured by the following components: – Capacitor (mGuard rs4000/rs2000 3G, mGuard industrial rs), – Battery (mGuard centerport, mGuard delta) or – Accumulator (mGuard rs4000/rs2000, mGuard pci^2 SD, mGuard delta^2, mGuard smart^2). In the case of the mGuard rs4000/rs2000, the accumulator lasts at least five days.

Management >> System Settings >> Time and Date[...]

Time-controlled activities

– **Time-controlled pick-up of configuration from a configuration server:**
  This is the case when the *Time Schedule* setting is selected under the *Management >> Central Management*, *Configuration Pull* menu item for the **Pull Schedule** setting (see “Management >> Configuration Profiles” on page 74, “Configuration Pull” on page 91).
– **Interruption of the connection at a certain time using PPPoE network mode:**
  This is the case when **Network Mode** is set to PPPoE under the *Network >> Interfaces, General* menu item, and **Automatic Re-connect** is set to Yes (see 6.1 “Network >> Interfaces”, ““Router” network mode, “PPPoE” router mode” on page 127).
– **Acceptance of certificates when the system time has not yet been synchronized:**
  This is the case when the *Wait for synchronization of the system time* setting is selected under the Authentication >> Certificates, Certificate settings menu item for the **Check the validity period of certificates and CRLs** option (see “Authentication >> Certificates” and “Certificate settings” on page 195).
– **CIFS integrity checking:**
  The regular, automatic check of the network drives is only started when the mGuard has a valid time and date (see the following section).

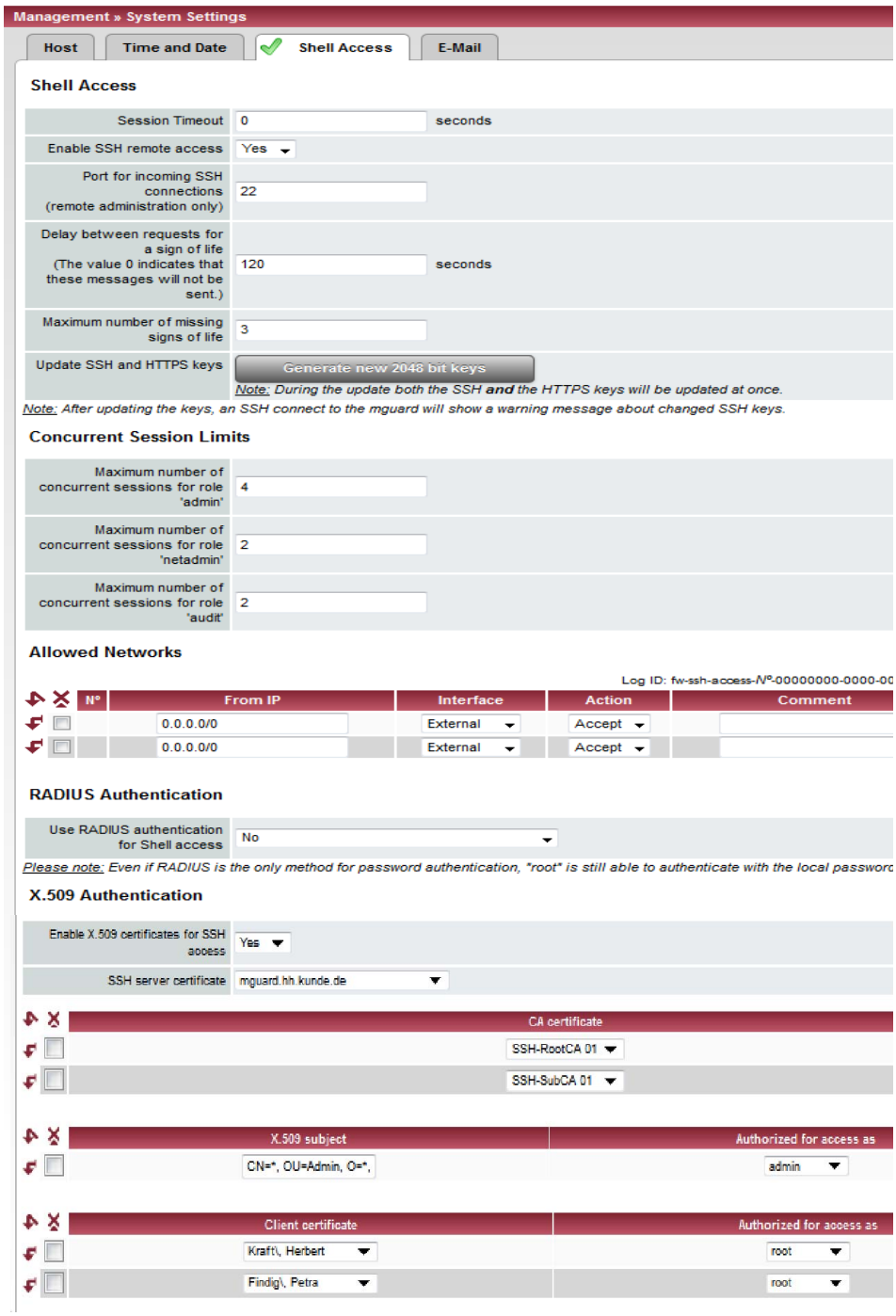
The system time can be set or synchronized by various events:

– **Synchronized by hardware clock**: The mGuard has a built-in clock, which has been synchronized with the current time at least once. A synchronized built-in clock ensures that the mGuard has a synchronized system time even after a restart.
– **Synchronized manually:** The administrator has defined the current time for the mGuard runtime by making a corresponding entry in the **Local system time** field.
– **Synchronized by file system time-stamp:** The administrator has set the **Time-stamp in filesystem** setting to *Yes*, and has either transmitted the current system time to the mGuard via NTP (see below under *NTP Server*) or has entered it under **Local system time**. The system time of the mGuard is then synchronized using the time stamp after a restart (even if it has no built-in clock and is set exactly again afterwards via NTP).
– **Synchronized by Network Time Protocol NTP:** The administrator has activated NTP time synchronization under **NTP Server**, has entered the address of at least one NTP server, and the mGuard has established a connection with at least one of the specified NTP servers. If the network is working correctly, this occurs a few seconds after a restart. The display in the **NTP State** field may only change to “synchronized” much later (see the explanation below under **NTP State**).
– **Synchronized by GPS data:** The mGuard rs4000/rs2000 3G can set and synchronize the system time via the positioning system (GPS/GLONASS) (under “Network >> Mobile Network >> Positioning system”).

Management >> System Settings >> Time and Date[...]		
	Local system time	Here you can set the time for the mGuard, if no NTP server has been set up or the NTP server cannot be reached. You should also set the system time if the menu item “Update System time” is set to “Yes” under the positioning system (under “Network >> Mobile Network >> Positioning system”). The date and time are specified in the format YYYY.MM.DD-HH:MM:SS: YYYY Year MM Month DD Day HH Hour MM Minute SS Second
	Timezone in POSIX.1 notation	If a current local time (that differs from Greenwich Mean Time) is to be displayed under *Current system time*, you must enter the number of hours that your local time is ahead of or behind Greenwich Mean Time. **Example**: in Berlin, the time is one hour ahead of GMT. Therefore, enter: CET-1. In New York, the time is five hours behind Greenwich Mean Time. Therefore, enter: CET+5. The only important thing is the -1, -2 or +1, etc. value as only these values are evaluated – not the preceding letters. They can be “CET” or any other designation, such as “UTC”. If you wish to display Central European Time (e.g., for Germany) and have it automatically switch to/from daylight saving time, enter: CET-1CEST,M3.5.0,M10.5.0/3
	Time-stamp in filesystem	If this option is set to **Yes**, the mGuard writes the current system time to its memory every two hours. If the mGuard is switched off and then on again, a time from this two-hour time slot is displayed, not a time on January 1, 2000.
NTP Server	(NTP - Network Time Protocol) The mGuard can act as the NTP server for computers that are connected to its LAN port. In this case, the computers should be configured so that the local address of the mGuard is specified as the NTP server address. If the mGuard is operated in *Stealth* mode, the management IP address of the mGuard (if this is configured) must be used for the computers, or the IP address 1.1.1.1 must be entered as the local address of the mGuard. For the mGuard to act as the NTP server, it must obtain the current date and the current time from an NTP server (= time server). To do this, the address of at least one NTP server must be specified. This feature must also be activated.	

Management >> System Settings >> Time and Date[...]		
	Enable NTP time synchronization	Once the NTP is activated, the mGuard obtains the date and time from one or more time server(s) and synchronizes itself with it or them. Initial time synchronization can take up to 15 minutes. During this time, the mGuard continuously compares the time data of the external time server and that of its own time so that this can be adjusted as accurately as possible. Only then the mGuard can act as the NTP server for the computers connected to its LAN interface and provide them with the system time. An initial time synchronization with the external time server is performed after every booting process, unless the mGuard has a built-in clock (for *mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard pci² SD, mGuard delta²* and for *mGuard smart²)*. After initial time synchronization, the mGuard regularly compares the system time with the time servers. Fine adjustment of the time is usually only made in the second range.
	NTP State	Displays the current NTP status. Shows whether the NTP server running on the mGuard has been synchronized with the configured NTP servers to a sufficient degree of accuracy. If the system clock of the mGuard has never been synchronized prior to activation of NTP time synchronization, then synchronization can take up to 15 minutes. The NTP server still changes the mGuard system clock to the current time after a few seconds, as soon as it has successfully contacted one of the configured NTP servers. The system time of the mGuard is then regarded as synchronized. Fine adjustment of the time is usually only made in the second range.
	NTP Server	Enter one or more time servers from which the mGuard should obtain the current time. If several time servers are specified, the mGuard will automatically connect to all of them to determine the current time.

4.1.3 Shell Access



Displayed when *Enable X.509 certificates for SSH access* is set to **Yes**

The mGuard must not be simultaneously configured via the web access, shell access, or SNMP. Simultaneous configuration via the different access methods might lead to unexpected results.

Management >> System Settings >> Shell Access

Shell Access

When SSH remote access is enabled, the mGuard can be configured **from remote computers** using the command line.

This option is disabled by default.

NOTE: If remote access is enabled, ensure that secure passwords are defined for *root* and *admin*.

Make the following settings for SSH remote access:

Session Timeout (seconds)

Specifies after what period of inactivity (in seconds) the session is automatically terminated, i.e., automatic logout. When set to 0 (default settings), the session is not terminated automatically.

The specified value is also valid for shell access via the serial interface instead of via the SSH protocol.

The effects of the “Session Timeout” field settings are temporarily ineffective if processing of a shell command exceeds the number of seconds set.

In contrast, the connection can also be aborted if it is no longer able to function correctly, see “Delay between requests for a sign of life” on page 42.

Enable SSH remote access

If you want to enable SSH remote access, set this option to **Yes**. *Internal* SSH access (i.e., from the directly connected LAN or from the directly connected computer) can be enabled independently of this setting.

The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access options on the mGuard.

Management >> System Settings >> Shell Access [...]		
	Port for incoming SSH connections (remote administration only)	Default: 22 If this port number is changed, the new port number only applies for access via the *External, External 2, VPN*, and *Dial-in* interface. Port number 22 still applies for internal access. The remote partner that implements remote access may have to specify the port number defined here during login. Example: If this mGuard can be accessed over the Internet via address 123.124.125.21 and default port number 22 has been specified for remote access, you may not need to enter this port number in the SSH client (e.g., PuTTY or OpenSSH) of the remote partner. If a different port number has been set (e.g., 2222), this must be specified, e.g.: ssh -p 2222 123.124.125.21
	Delay between requests for a sign of life	Default: 120 seconds Values from 0 to 3600 seconds can be set. Positive values indicate that the mGuard is sending a query to the partner within the encrypted SSH connection to find out whether it can still be accessed. The request is sent if no activity was detected from the partner for the specified number of seconds (e.g., due to network traffic within the encrypted connection). The value entered relates to the functionality of the encrypted SSH connection. As long as the functions are working properly, the SSH connection is not terminated by the mGuard as a result of this setting, even when the user does not perform any actions during this time. Because the number of simultaneously open sessions is limited (see *Concurrent Session Limits*), it is important to terminate sessions that have expired. Therefore, the request for a sign of life is preset to 120 seconds in the case of Version 7.4.0 or later. If a maximum of three requests for a sign of life are issued, this causes an expired session to be detected and removed after six minutes. In previous versions, the preset was “0”. This means that no requests for a sign of life are sent. If it is important not to generate additional traffic, you can adjust the value. When the setting “0” is made in conjunction with “*Concurrent Session Limits*”, subsequent access may be blocked if too many sessions are interrupted but not closed as a result of network errors.

Management >> System Settings >> Shell Access [...]

	Maximum number of missing signs of life	Specifies the maximum number of times a sign of life request to the partner may remain unanswered. For example, if a sign of life request should be made every 15 seconds and this value is set to 3, the SSH connection is deleted if a sign of life is still not detected after approximately 45 seconds.
	Update SSH and HTTPS keys	**Generate new 2048-bit keys** Keys that have been generated using an older firmware might be weak and should be renewed. • Click on this button to generate a new key. • Observe the fingerprints of the new keys generated. • Login via HTTPS and compare the certificate information provided by the browser.
Concurrent Session Limits	In the case of administrative access to the mGuard via SSH, the number of simultaneous sessions is limited, depending on the predefined user. Approximately 0.5 Mbytes of memory space are required for each session. The “root” user has unrestricted access. In the case of administrative access via another user *(admin, netadmin,* and *audit),* the number of simultaneous sessions is restricted. You can specify the number here. The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager. The restriction does not affect existing sessions; it only affects newly established access instances.	
	Maximum number of concurrent sessions for role “admin”	2 to 2147483647 At least two simultaneously permitted sessions are required for “admin” to prevent it from having its access blocked.
	Maximum number of concurrent sessions for role “netadmin”	0 to 2147483647 When “0” is set, no session is permitted. The “netadmin” user is not necessarily used.
	Maximum number of concurrent sessions for role “audit”	0 to 2147483647 When “0” is set, no session is permitted. The “audit” user is not necessarily used.
Allowed Networks		

Management >> System Settings >> Shell Access [...]

Lists the firewall rules that have been set up. These apply for incoming data packets of an SSH remote access attempt.

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

The rules specified here only take effect if **Enable SSH remote access** is set to **Yes**. *Internal* access is also possible when this option is set to **No**. A firewall rule that would refuse *Internal* access does therefore not apply in this case.

The following options are available:

From IP

Enter the address of the computer or network from which remote access is permitted or forbidden in this field.

The following options are available:

IP address: **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format, see “CIDR (Classless Inter-Domain Routing)” on page 24.

Interface

External/Internal/External 2/VPN/Dial-in

External 2 and *Dial-in* are only for devices with a serial interface, see “Network >> Interfaces” on page 105.

Specifies to which interface the rule should apply.

If no rules are set or if no rule applies, the following default settings apply:

SSH access is permitted via *Internal*, *VPN*, and *Dial-in*. Access via External and External 2 is refused.

Specify the access options according to your requirements.

NOTE: If you want to refuse access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as an action.

To prevent your own access being blocked, you may have to permit access simultaneously via another interface explicitly with *Accept* before clicking on the **Apply** button to activate the new setting. Otherwise, if your access is blocked, you must carry out the recovery procedure.

Management >> System Settings >> Shell Access [...]		
	Action	Options: – **Accept** means that the data packets may pass through. – **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.) – **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default setting)

Management >> System Settings >> Shell Access [...]

RADIUS Authentication

This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.

Use RADIUS authentication for Shell access

If set to **No**, the passwords of users who log in via shell access are checked via the local database on the mGuard.

Select **Yes** to enable users to be authenticated via a RADIUS server. This also applies for users who want to access the mGuard via shell access using SSH or a serial console. The password is only checked locally in the case of predefined users *(root, admin, netadmin,* and *audit)*.

The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager.

Under **X.509 Authentication**, if you set **Enable X.509 certificates for SSH access** to **Yes**, the X.509 authentication procedure can be used as an alternative. Which procedure is actually used by the user depends on how the user uses the SSH client.

When setting up a RADIUS authentication for the first time, select **Yes**.

You should only select **As only method for password authentication** if you are an experienced user, as doing so could result in all access to the mGuard being blocked.

If you do intend to use the **As only method for password authentication** option when setting up RADIUS authentication, we recommend that you create a “Customized Default Profile” which resets the authentication method.

The predefined users *(root, admin, netadmin,* and *audit)* are then no longer able to log in to the mGuard via SSH or serial console.

There is one exception: it is still possible to perform authentication via an externally accessible serial console by correctly entering the local password for the *root* user name.

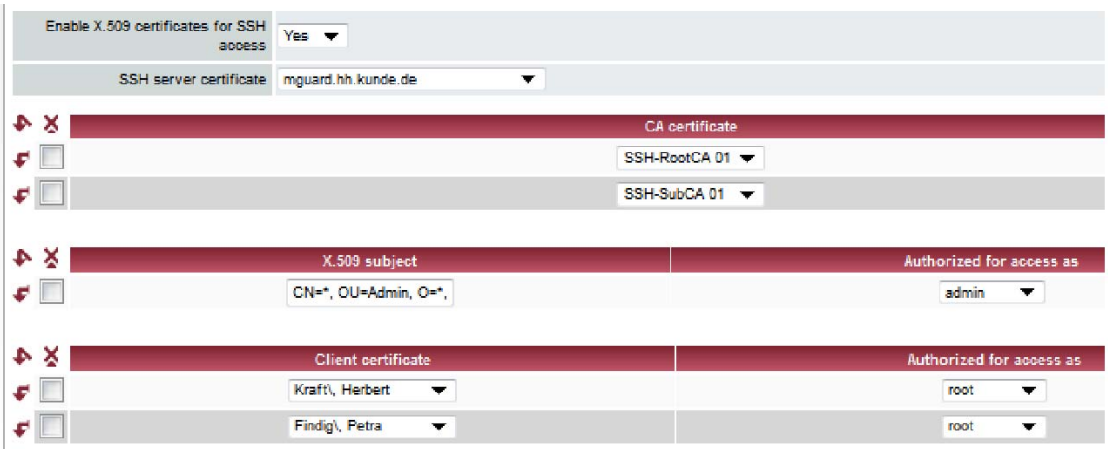
X.509 Authentication

X.509 certificates for SSH clients

The mGuard supports the authentication of SSH clients using X.509 certificates. It is sufficient to configure CA certificates that are required for the establishment and validity check of a certificate chain. This certificate chain must exist between the CA certificate on the mGuard and the X.509 certificate shown to the SSH client (see “Shell Access” on page 40).

If the validity period of the client certificate is checked by the mGuard (see “Certificate settings” on page 195), new CA certificates must be configured on the mGuard at some point. This must take place before the SSH clients use their new client certificates.

If the CRL check is activated (under *Authentication* >> *Certificates* >> *Certificate settings),* one URL (where the corresponding CRL is available) must be maintained for each CA certificate. The URL and CRL must be published before the mGuard uses the CA certificates in order to confirm the validity of the certificates shown by the VPN partners.



Management >> System Settings >> Shell Access

X.509 Authentication

This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.

Enable X.509 certificates for SSH access

- If **No** is selected, then only conventional authentication methods (user name and password or private and public keys) are permitted, not the X.509 authentication method.
- If **Yes** is selected, then the X.509 authentication method can be used in addition to conventional authentication methods (as also used for **No**).
- If **Yes** is selected, the following must be specified:
  - How the mGuard authenticates itself to the SSH client according to X.509, see **SSH server certificate (1)**
  - How the mGuard authenticates the remote SSH client according to X.509, see **SSH server certificate (2)**

Management >> System Settings >> Shell Access[...]

SSH server certificate (1)

Specifies how the mGuard identifies itself to the SSH client.

Select one of the machine certificates from the list or the *None* entry.

None:

When *None* is selected, the SSH server of the mGuard does not authenticate itself to the SSH client via the X.509 certificate. Instead, it uses a server key and thus behaves in the same way as older versions of the mGuard.

If one of the machine certificates is selected, this is also offered to the SSH client. The client can then decide whether to use the conventional authentication method or the method according to X.509.

The selection list contains the machine certificates that have been loaded on the mGuard under the *Authentication >> Certificates* menu item (see Page 190).

SSH server certificate (2)

Specifies how the mGuard authenticates the SSH client

The following definition relates to how the mGuard verifies the authenticity of the SSH client.

The table below shows which certificates must be provided for the mGuard to authenticate the SSH client if the SSH client shows one of the following certificate types when a connection is established:

– A certificate signed by a CA
– A self-signed certificate

For additional information about the table, see “Authentication >> Certificates” .

Authentication for SSH

The partner shows the following:	Certificate (specific to individual), **signed by CA**	Certificate (specific to individual), **self-signed**
The mGuard authenticates the partner using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner PLUS (if required) Remote certificates, **if** used as a filter	Remote certificate

According to this table, the certificates that must be provided are the ones the mGuard uses to authenticate the relevant SSH client.

The following instructions assume that the certificates have already been correctly installed on the mGuard (see *"Authentication >> Certificates"*).

If the use of revocation lists (CRL checking) is activated under the *"Authentication >> Certificates" , Certificate settings* menu item, each certificate signed by a CA that is "shown" by SSH clients is checked for revocations.

Management >> System Settings >> Shell Access

CA certificate

This configuration is only necessary if the SSH client shows a certificate signed by a CA.

All CA certificates required by the mGuard to form the chain to the relevant root CA certificate with the certificates shown by the SSH client must be configured.

The selection list contains the CA certificates that have been loaded on the mGuard under the *Authentication >> Certificates* menu item.

X.509 subject

Enables a filter to be set in relation to the contents of the *Subject* field in the certificate shown by the SSH client. It is then possible to limit or enable access for SSH clients, which the mGuard would accept based on certificate checks:

– Limited access to certain *subjects* (i.e., individuals) and/or to *subjects* that have certain attributes or
– Access enabled for all subjects (see glossary under *"Subject, certificate" on page 360*).

The *X.509 subject* field must not be left empty.

Management >> System Settings >> Shell Access[...]

Access enabled for all subjects (i.e., individuals):

An * (asterisk) in the *X.509 subject* field can be used to specify that all subject entries in the certificate shown by the SSH client are permitted. It is then no longer necessary to identify or define the subject in the certificate.

Limited access to certain subjects (i.e., individuals) or to subjects that have certain attributes:

In the certificate, the certificate owner is specified in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an object identifier (e.g., 132.3.7.32.1) or, more commonly, as an abbreviation with a corresponding value.

Example: CN=John Smith, O=Smith and Co., C=US

If certain subject attributes have very specific values for the acceptance of the SSH client by the mGuard, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the ***** (asterisk) wildcard.

Example: CN=*, O=*, C=US (with or without spaces between attributes)

In this example, the attribute “C=US” must be entered in the certificate under “Subject”. It is only then that the mGuard would accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have any value.

If a subject filter is set, the number (but not the order) of the specified attributes must correspond to that of the certificates for which the filter is to be used.

Please note that the filter is case-sensitive.

Several filters can be set and their sequence is irrelevant.

Authorized for access as

All users/root/admin/netadmin/audit

Additional filter which specifies that the SSH client has to be authorized for a specific administration level in order to gain access.

When establishing a connection, the SSH client shows its certificate and also specifies the system user for which the SSH session is to be opened (*root, admin, netadmin, audit*). Access is only granted if the entries match those defined here.

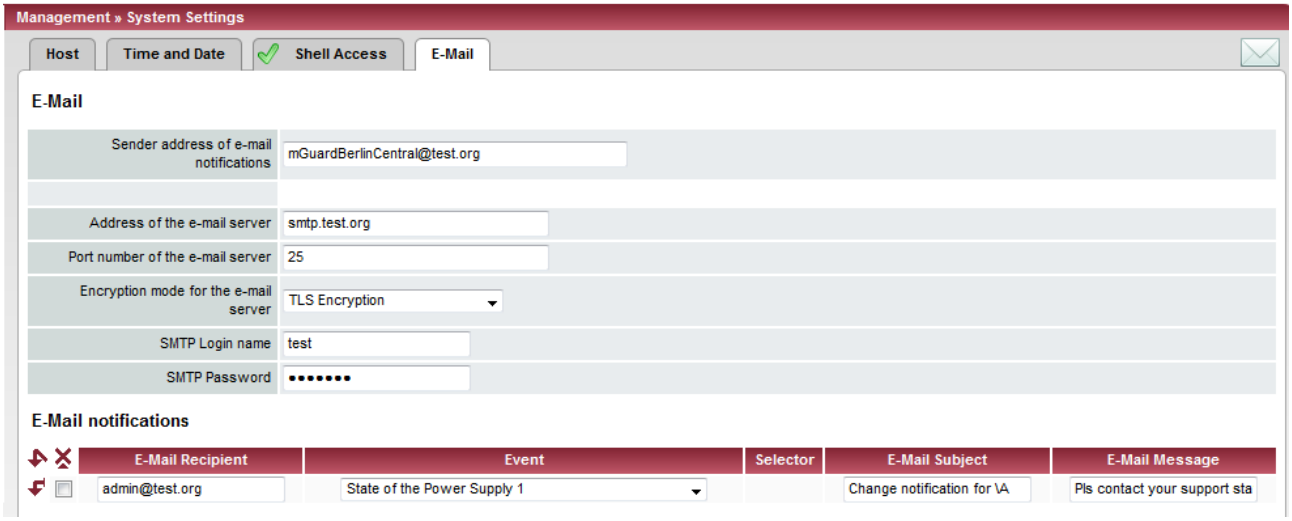
Access for all listed system users is possible when *All users* is set.

The *netadmin* and *audit* setting options relate to access rights with the mGuard device manager.

Management >> System Settings >> Shell Access[...]

Client certificate	Configuration is required in the following cases: – SSH clients each show a self-signed certificate. – SSH clients each show a certificate signed by a CA. Filtering should take place: access is only granted to a user whose certificate copy is installed on the mGuard as the remote certificate and is provided to the mGuard in this table as the *Client certificate*. This filter is not subordinate to the *Subject* filter. It resides on the same level and is allocated a logical OR function with the Subject filter. The entry in this field defines which remote certificate the mGuard should adopt in order to authenticate the partner (SSH client). The remote certificate can be selected from the selection list. The selection list contains the remote certificates that have been loaded on the mGuard under the *"Authentication >> Certificates"* menu item.
Authorized for access as	All users/root/admin/netadmin/audit Filter which specifies that the SSH client has to be authorized for a specific administration level in order to gain access. When establishing a connection, the SSH client shows its certificate and also specifies the system user for which the SSH session is to be opened (*root, admin, netadmin, audit*). Access is only granted if the entries match those defined here. Access for all listed system users is possible when *All users* is set. The *netadmin* and *audit* setting options relate to access rights with the mGuard device manager.

4.1.4 E-Mail



Management >> System Settings >> E-Mail

E-Mail (Make sure that the e-mail settings for the mGuard are correctly configured)	**Sender address of e-mail notifications**	E-mail address, which is displayed as the sender from mGuard.
	Address of the e-mail server	Address of the e-mail server
	Port number of the e-mail server	Port number of the e-mail server
	Encryption mode for the e-mail server	**No Encryption / TLS Encryption / TLS Encryption with StartTLS** Encryption mode for the e-mail server
	SMTP Login name	User name
	SMTP Password	Password for the e-mail server
E-Mail notifications	Any e-mail recipients can be linked with predefined events and a freely definable message. The list is processed from top to bottom.	
	E-Mail recipient	Specifies the e-mail address.
	Event	When the selected event occurs or the event is configured for the first time, the linked recipient address is selected and the event is sent to them via e-mail. An e-mail message can also be stored and sent. Some of the events listed depend on the hardware used. A complete list of all events can be found at “Event table” on page 53.
	Selector	A configured VPN connection can be selected here, which is monitored via e-mail.

Management >> System Settings >> E-Mail [...]		
	E-Mail Subject	Text appears in the subject line of the e-mail The text is freely definable. You can use blocks from the events table which can be inserted as wildcards in plain text (\A and \V) or in machine-readable form (\a and v\).
	E-Mail Message	Here you can enter the text that is sent as the e-mail body. The text is freely definable. You can use blocks from the events table which can be inserted as wildcards in plain text (\A and \V) or in machine-readable form (\a and v\).

Table 4-1 Event table

Plain text		**Machine-readable**	
\A = event	**\V = value**	**\a = event**	**\v = value**
State of the External Configuration Storage ECS	Not present	/ecs/status	1
	Removed		2
	Present and in sync		3
	Not in sync		4
	Generic Error		8
Validity of the positional data	Positioning data not valid	/gps/valid	no
	Positioning data valid		yes
Telephone number of an incoming call		/gsm/incoming_call	
Telephone number and message of an incoming text message		/gsm/incoming_sms	
Roaming state of the mobile network engine	Registered to home network	/gsm/roaming	no
	Registered to foreign network		yes
	Not registered		unknown
Registration state to the mobile network	Not registered to mobile network	/gsm/service	no
	Registered to mobile network		yes
Currently selected SIM slot	Using SIM 1	/gsm/selected_sim	1
	Using SIM 2		2
	SIM interface disabled		0
Mobile network fallback SIM activity	Normal operation (Primary SIM)	/gsm/sim_fallback	no
	Fallback mode (Secondary SIM)		yes
Mobile network probes	The network probes are disabled	/gsm/network_probe	disabled
	The network probes are enabled		enabled
	The network probes failed		failed
	The network probes succeeded		succeeded

Table 4-1 Event table

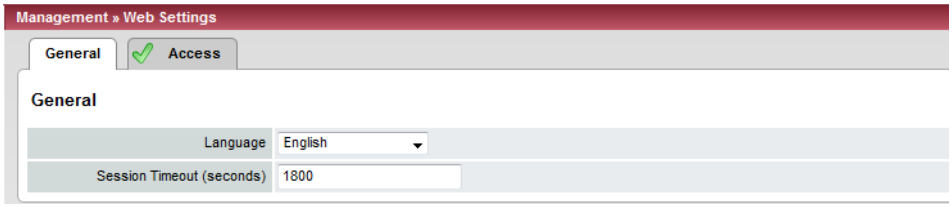
Plain text		Machine-readable	
\A = event	**\V = value**	**\a = event**	**\v = value**
State of the Alarm output	Alarm output closed [OK]	/ihal/contact	close
	Alarm output is open [FAILURE]		open
Reason for activating the Alarm output	No alarm	/ihal/contactreason	
	No network link on external interface		link_ext
	No network link on internal interface		link_int
	Power supply 1 out of order		psu1
	Power supply 2 out of order		psu2
	Board temperature exceeding configured bounds		temp
	Redundancy connectivity check failed		check
	The internal modem is offline		modem
	No network link on LAN2		link_swp0
	No network link on LAN3		link_swp1
	No network link on LAN1		link_swp2
	No network link on LAN4		link_swp3
	No network link on LAN5		link_swp4
	No network link on DMZ		link_dmz
State of Power Supply 1	Power supply 1 working	/ihal/power/psu1	ok
	Power supply 1 out of order		fail
State of Power Supply 2	Power supply 2 working	/ihal/power/psu2	ok
	Power supply 2 out of order		fail
State of the Input/CMD 1	Service input 1 activated	/ihal/service/cmd1	on
	Service input 1 deactivated		off
State of the Input/CMD 3	Service input 2 activated	/ihal/service/cmd2	on
	Service input 2 deactivated		off
State of the Input/CMD 3	Service input 3 activated	/ihal/service/cmd3	on
	Service input 3 deactivated		off
Board temperature state	Temperature OK	/ihal/temperature/board_alarm	ok
	Temperature too hot		hot
	Temperature too cold		cold
Temporary state of the secondary external interface	On standby	/network/ext2up	no
	Temporarily up		yes
State of the modem	Offline	/network/modem/state	offline
	Dialing		dialing
	Online		online
	Initialized waiting		init

Table 4-1 Event table

Plain text		Machine-readable	
\A = event	**\V = value**	**\a = event**	**\v = value**
Status of the redundancy subsystem	The redundancy controller starts up	/redundancy/status	booting
	The device does not (yet) have proper connectivity or cannot determine it for sure		faulty
	The device does not (yet) have proper connectivity or cannot determine it for sure and waits for a restarting component		faulty_waiting
	The device has an empty or outdated firewall or VPN state information which it wants to resynchronize		outdated
	The device has an empty or outdated firewall or VPN state information which it wants to resynchronize and waits for a restarting component		outdated_waiting
	The device is on standby		on_standby
	The device is on standby and waits for a restarting component		on_standby_waiting
	The device becomes active		becomes_active
	The device is actively forwarding and filtering network traffic		active
	The device is actively forwarding and filtering network traffic and waits for a restarting component		active_waiting
	The device transitions to the hot standby state		becomes_standby
VPN Connection Preparation state	Stopped	/vpn/con/*/armed	no
	Started		yes
VPN Connection IPsec SA state	No IPsec SAs established	/vpn/con/*/ipsec	down
	Not all IPSec SAs established		some
	All IPSec SAs established		up
Activation state of a Firewall rule record	The state of the firewall rule record has changed.	/fwrules/*/state	inactive
			active

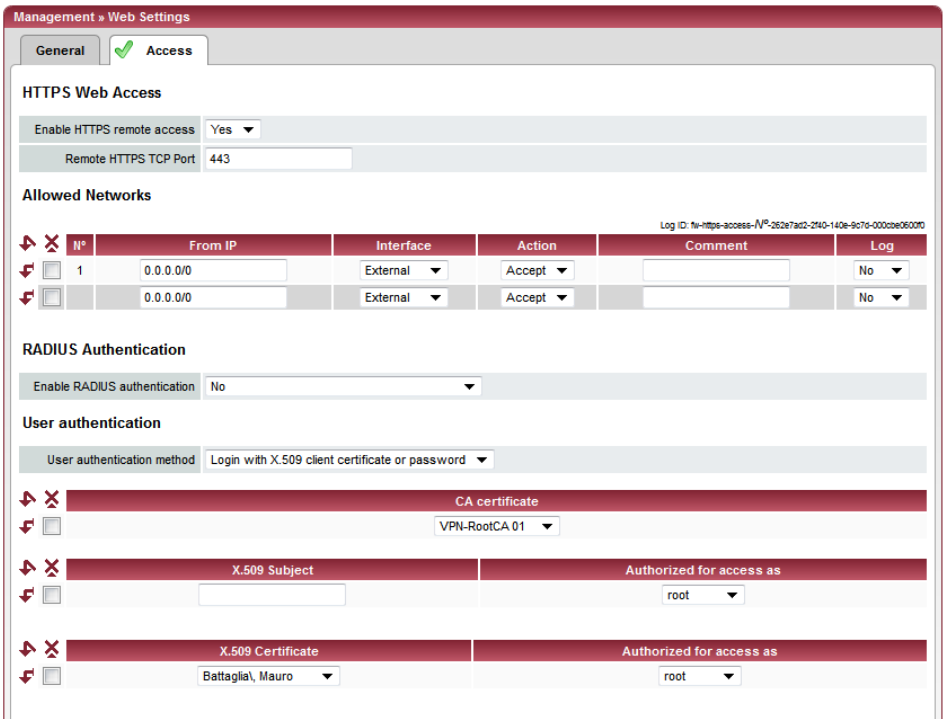
4.2 Management >> Web Settings

4.2.1 General



Management >> Web Settings >> General		
General	**Language**	If **(automatic)** is selected in the list of languages, the device uses the language setting of the computer's browser.
	Session Timeout (seconds)	Specifies the period of inactivity (in seconds) after which the user will be automatically logged out of the mGuard web interface. Possible values: 15 to 86400 (= 24 hours)

4.2.2 Access



Only displayed when *Login with X.509 user certificate* is selected

The mGuard must not be simultaneously configured via the web access, shell access, or SNMP. Simultaneous configuration via the different access methods might lead to unexpected results.

When web access via HTTPS protocol is enabled, the mGuard can be configured **from a remote computer** using its web-based administrator interface. This means that a browser on the remote computer is used to configure the mGuard.

This option is disabled by default.

NOTE: If remote access is enabled, ensure that secure passwords are defined for *root* and *admin*.

To enable HTTPS remote access, make the following settings:

Management >> Web Settings >> Access		
HTTPS Web Access	**Enable HTTPS remote access: Yes/No**	If you want to enable HTTPS remote access, set this option to **Yes**. *Internal* HTTPS remote access (i.e., from the directly connected LAN or from the directly connected computer) can be enabled independently of this setting. The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access options on the mGuard. In addition, the authentication rules under **User authentication** must be set, if necessary.
	Remote HTTPS TCP Port (remote administration only)	Default: 443 If this port number is changed, the new port number only applies for access via the *External, External 2, VPN*, and *Dial-in* interface. Port number 443 still applies for internal access. The remote partner that implements remote access may have to specify the port number defined here after the IP address during entry of the address. **Example:** if this mGuard can be accessed over the Internet via address 123.124.125.21 and port number 443 has been specified for remote access, you do not need to enter this port number after the address in the web browser of the remote partner. If a different port number is used, it should be entered after the IP address, e.g.,: https://123.124.125.21:442/ The mGuard authenticates itself to the partner, in this case the browser of the user, using a self-signed machine certificate. This is a unique certificate issued by Innominate for each mGuard. This means that every mGuard device is delivered with a unique, self-signed machine certificate.
	Update SSH and HTTPS keys	**Generate new 2048-bit keys** Keys that have been generated using a older firmware might be weak and should be renewed. • Click on this button to generate a new key. • Observe the fingerprints of the new keys generated. • Login via HTTPS and compare the certificate information provided by the browser.

Management >> Web Settings >> Access[...]

Allowed Networks

Lists the firewall rules that have been set up. These apply for incoming data packets of an HTTPS remote access attempt.

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

The rules specified here only take effect if **Enable HTTPS remote access** is set to **Yes**. *Internal* access is also possible when this option is set to **No**. A firewall rule that would refuse *Internal* access does therefore not apply in this case.

The following options are available:

From IP

Enter the address of the computer or network from which remote access is permitted or forbidden in this field.

IP address: **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format – see “CIDR (Classless Inter-Domain Routing)” on page 24.

Interface

External/Internal/External 2/VPN/Dial-in[1]

Specifies to which interface the rule should apply.

If no rules are set or if no rule applies, the following default settings apply:

HTTPS access is permitted via *Internal, VPN*, and *Dial-in*. Access via *External* and *External 2* is refused.

Specify the access options according to your requirements.

If you want to refuse access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as an action. **To prevent your own access being blocked**, you may have to permit access simultaneously via another interface explicitly with *Accept* before clicking on the **Apply** button to activate the new setting. Otherwise, if your access is blocked, you must carry out the recovery procedure.

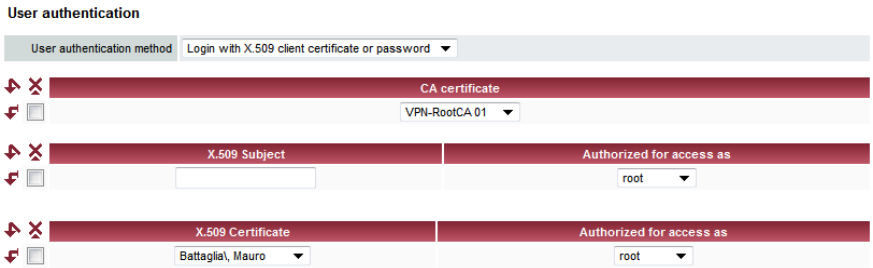
Management >> Web Settings >> Access[...]		
	Action	– **Accept** means that the data packets may pass through. – **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.) – **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	**Freely selectable comment for this rule.**
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default setting)
RADIUS Authentication This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.	**Enable RADIUS authentication**	If set to **No**, the passwords of users who log in via HTTPS are checked via the local database. The **User authentication method** can only be set to **Login restricted to X.509 client certificate** if **No** is selected. Select **Yes** to enable users to be authenticated via the RADIUS server. The password is only checked locally in the case of predefined users (*root*, *admin*, *netadmin*, *audit,* and *user)*. The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager. You should only select **As only method for password authentication** if you are an experienced user, as doing so could result in all access to the mGuard being blocked. When setting up a RADIUS authentication for the first time, select **Yes**. If you do intend to use the **As only method for password authentication** option when setting up RADIUS authentication, we recommend that you create a “Customized Default Profile” which resets the authentication method. If you have selected RADIUS authentication as the only method for checking the password, it may no longer be possible to access the mGuard. For example, this may be the case if you set up the wrong RADIUS server or convert the mGuard. The predefined users (*root*, *admin*, *netadmin*, *audit,* and *user)* are then no longer accepted.

1 *External 2* and *Dial-in* are only for devices with a serial interface (see “Network >> Interfaces” on page 105).

Management >> Web Settings >> Access

User authentication

This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.



Defines how the local mGuard authenticates the remote partner

User authentication method

Login with password

Specifies that the remote mGuard user must use a password to log into the mGuard. The password is specified under the *Authentication >> Administrative Users* menu (see Page 181). The option of RADIUS authentication is also available (see Page 187).

Depending on which user ID is used to log in (user or administrator password), the user has the right to operate and/or configure the mGuard accordingly.

Login with X.509 client certificate or password

– User authentication is by means of login with a password (see above) or
– The user's browser authenticates itself using an X.509 certificate and a corresponding private key. Additional details must be specified below.

The use of either method depends on the web browser of the remote user. The second option is used when the web browser provides the mGuard with a certificate.

Login restricted to X.509 client certificate

The user's browser must use an X.509 certificate and the corresponding private key to authenticate itself. Additional details must be specified here.

Before enabling the *Login restricted to X.509 client certificate* option, you must first select and test the *Login with X.509 client certificate or password* option.

Only switch to *Login restricted to X.509 client certificate* when you are sure that this setting works. **Otherwise your access could be blocked.**

Always take this precautionary measure when modifying settings under **User authentication**.

If the following **User authentication methods** are defined:

– Login restricted to X.509 client certificate
– Login with X.509 client certificate or password

You must then specify how the mGuard authenticates the remote user according to X.509.

The table below shows which certificates must be provided for the mGuard to authenticate the user (access via HTTPS) if the user or their browser shows one of the following certificate types when a connection is established:

– A certificate signed by a CA
– A self-signed certificate

For additional information about the table, see “Authentication >> Certificates” on page 190.

X.509 authentication for HTTPS

The partner shows the following:	Certificate (specific to individual), **signed by CA**[1]	Certificate (specific to individual), **self-signed**
The mGuard authenticates the partner using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner PLUS (if required) Remote certificates, **if** used as a filter	Remote certificate

[1] The partner can additionally provide sub-CA certificates. In this case, the mGuard can form the set union for creating the chain from the CA certificates provided and the self-configured CA certificates. The corresponding root certificate must always be available on the mGuard.

According to this table, the certificates that must be provided are the ones the mGuard uses to authenticate a remote user (access via HTTPS) or their browser.

The following instructions assume that the certificates have already been correctly installed on the mGuard (see “Authentication >> Certificates” on page 190).

If the use of revocation lists (CRL checking) is activated under the Authentication >> Certificates, *Certificate settings* menu item, each certificate signed by a CA that is “shown” by the HTTPS clients must be checked for revocations.

Management >> Web Settings >> Access

CA certificate

This configuration is only necessary if the user (access via HTTPS) shows a certificate signed by a CA.

All CA certificates required by the mGuard to form the chain to the relevant root CA certificate with the certificates shown by the user must be configured.

If the browser of the remote user also provides CA certificates that contribute to forming the chain, then it is not necessary for these CA certificates to be installed on the mGuard and referenced at this point.

However, the corresponding root CA certificate must be installed on the mGuard and made available (referenced) in any case.

When selecting the CA certificates to be used or when changing the selection or the filter settings, you must first select and test the *Login with X.509 client certificate or password* option as the *User authentication method* before enabling the (new) setting.

Only switch to *Login restricted to X.509 client certificate* when you are sure that this setting works. **Otherwise your access could be blocked.**

Always take this precautionary measure when modifying settings under **User authentication**.

Management >> Web Settings >> Access [...]

X.509 Subject

Enables a filter to be set in relation to the contents of the *Subject* field in the certificate shown by the browser/HTTPS client.

It is then possible to limit or enable access for the browser/HTTPS client, which the mGuard would accept based on certificate checks:

– Limited access to certain *subjects* (i.e., individuals) and/or to *subjects* that have certain attributes or
– Access enabled for all subjects (see glossary under “Subject, certificate” on page 360).

The *X.509 Subject* field must not be left empty.

Access enabled for all subjects (i.e., individuals):

An * (asterisk) in the *X.509 Subject* field can be used to specify that all subject entries in the certificate shown by the browser/HTTPS client are permitted. It is then no longer necessary to identify or define the subject in the certificate.

Management >> Web Settings >> Access [...]

Limited access to certain subjects (i.e., individuals) and/or to subjects that have certain attributes:

In the certificate, the certificate owner is specified in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an object identifier (e.g., 132.3.7.32.1) or, more commonly, as an abbreviation with a corresponding value.

Example: CN=John Smith, O=Smith and Co., C=US

If certain subject attributes have very specific values for the acceptance of the browser by the mGuard, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the ***** (asterisk) wildcard.

Example: CN=*, O=*, C=US (with or without spaces between attributes)

In this example, the attribute “C=US” must be entered in the certificate under “Subject”. It is only then that the mGuard would accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have any value.

If a subject filter is set, the number (but not the order) of the specified attributes must correspond to that of the certificates for which the filter is to be used.

Please note that the filter is case-sensitive.

Several filters can be set and their sequence is irrelevant.

With HTTPS, the browser of the accessing user does not specify which user or administration rights it is using to log in. These access rights are assigned by setting filters here (under “Authorized for access as”).

This has the following result: if there are several filters that “let through” a certain user, then the first filter applies. The user is assigned the access rights as defined by this filter. This could differ from the access rights assigned to the user in the subsequent filters.

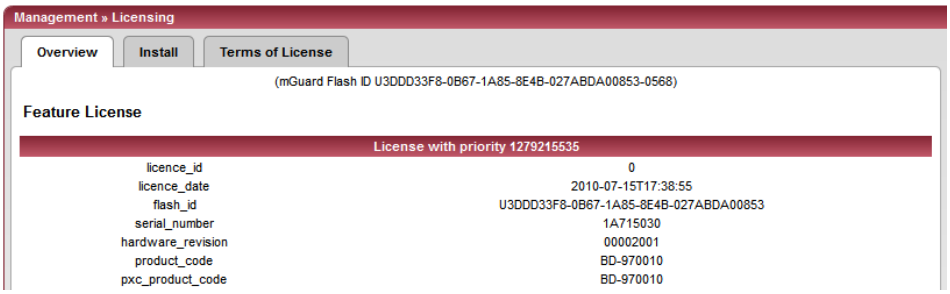
If remote certificates are configured as filters in the **X.509 Certificate** table column, then these filters have priority over the filter settings here.

Management >> Web Settings >> Access [...]		
	Authorized for access as	**All users/root/admin/netadmin/audit** Specifies which user or administrator rights are granted to the remote user. For a description of the *root, admin*, and *user* authorization levels, see “Authentication >> Administrative Users” on page 181. The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager.
	X.509 Certificate	Configuration is required in the following cases: – Remote users each show a self-signed certificate. – Remote users each show a certificate signed by a CA. Filtering should take place: access is only granted to a user whose certificate copy is installed on the mGuard as the remote certificate and is provided to the mGuard in this table as the *X.509 certificate*. If used, this filter has priority over the *Subject* filter in the table above. The entry in this field defines which remote certificate the mGuard should adopt in order to authenticate the partner (browser of the remote user). The remote certificate can be selected from the selection list. The selection list contains the remote certificates that have been loaded on the mGuard under the *Authentication* >> *Certificates* menu item.
	Authorized for access as	**root/admin/netadmin/audit/user** Specifies which user or administrator rights are granted to the remote user. For a description of the *root, admin*, and *user* authorization levels, see “Authentication >> Administrative Users” on page 181. The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager.

4.3 Management >> Licensing

You can obtain additional optional licenses from you authorized mGuard dealer.

4.3.1 Overview



With mGuard Version 5.0 or later, licenses remain installed even after the firmware is flashed.

However, licenses are still deleted when devices with older firmware versions are flashed to Version 5.0.0 or later. Before flashing, the license for using the new update must then first be obtained so that the required license file is available for the flashing process.

This applies to major release upgrades, e.g., from Version 4.x.y to Version 5.x.y to Version 6.x.y, etc.

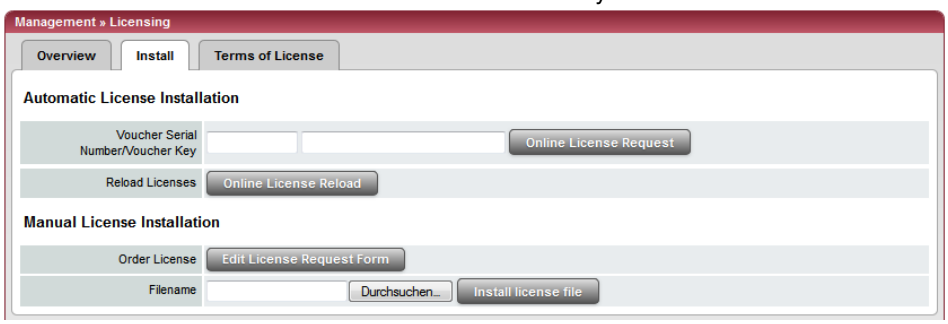
Management >> Licensing >> Overview		
Basic settings	**Feature License**	Shows which functions are included with the installed mGuard licenses, e.g., the number of possible VPN tunnels, whether remote logging is supported, etc.

4.3.2 Install

A VPN-1000 license can only be installed on the mGuard centerport.

Only an MRU and LFS license can be installed on the mGuard rs2000 (3G).

More functions can be added later to the mGuard license you have obtained. You will find a



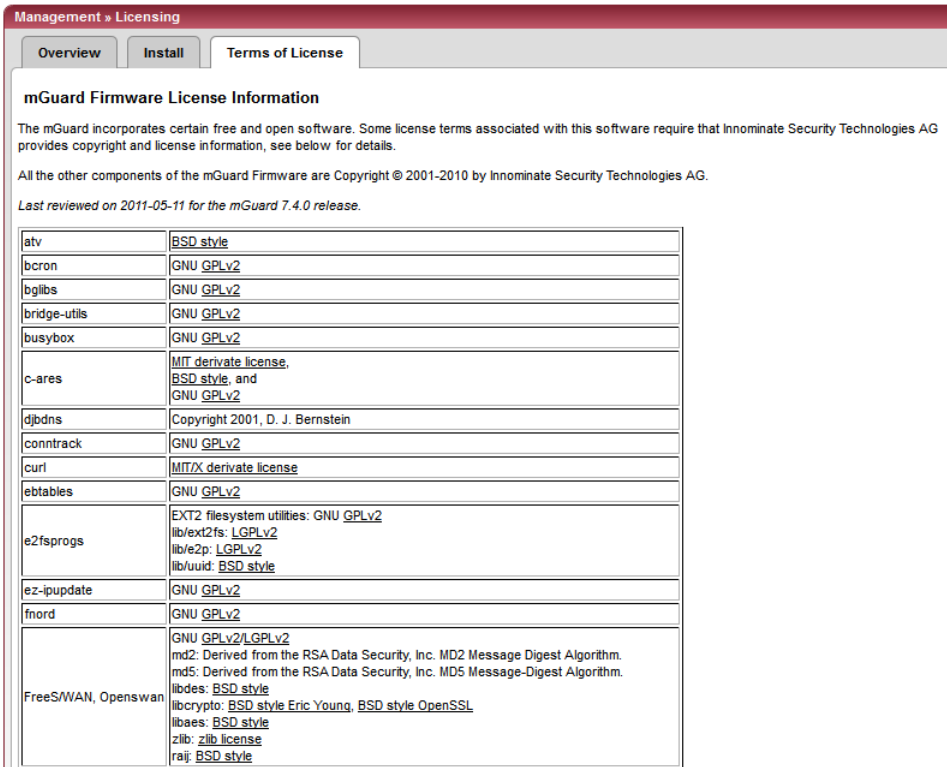
voucher serial number and a voucher key in the voucher included with the mGuard. The voucher can also be purchased separately.

It can be used to:

– Request the required feature license file
– Install the license file that you receive following this request

Management >> Licensing >> Install		
Automatic License Installation	**Voucher Serial Number/Voucher Key**	Enter the serial number printed on the voucher and the corresponding voucher key, then click on **Online License Request**. The mGuard now establishes a connection via the Internet and installs the corresponding license on the mGuard if the voucher is valid.
	Reload Licenses	This option can be used if the license installed on the mGuard has been deleted. Click on **Online License Reload**. The licenses that were previously issued for this mGuard are then retrieved from the server via the Internet and installed.
Manual License Installation	**Order License** **Filename**	After clicking on **Edit License Request Form**, an online form is displayed, which can be used to order the desired license. Enter the following information in the form: – **Voucher Serial Number**: the serial number printed on your voucher – **Voucher Key**: the voucher key on your voucher – **Flash ID:** this is entered automatically After sending the form, the license file is made available for download and can be installed on the mGuard in a further step. **Install license file** To install a license, first save the license file as a separate file on your computer, then proceed as follows: • Click on Browse... next to the *Filename* field. Select the file and open it so that the file name or path is displayed in the Filename field. • Then click on **Install license file**.

4.3.3 Terms of License



Lists the licenses of the external software used on the mGuard. The software is usually open-source software.

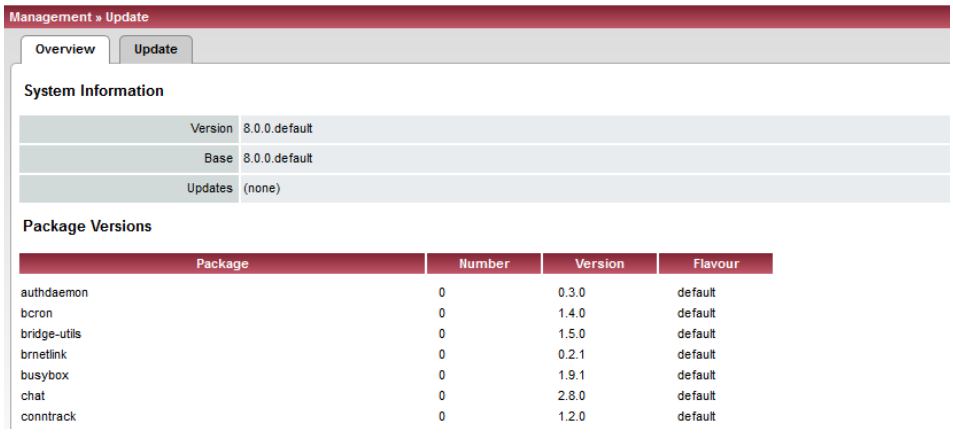
4.3.4 Management >> Update

With mGuard firmware Version 5.0.0 or later, a license must be obtained for the relevant device before a major release upgrade (e.g., from Version 4.x.y to Version 5.x.y or from Version 5.x.y to Version 6.x.y) can be installed.

The license must be installed on the device before updating the firmware (see “Management >> Licensing” on page 67 and “Install” on page 67).

Minor release upgrades (i.e., the same major version, e.g., within Version 5.x.y) can be installed without a license until further notice.

4.3.5 Overview



Management >> Update >> Overview		
System Information	**Version**	The current software version of the mGuard.
	Base	The software version that was originally used to flash this mGuard.
	Updates	List of updates that have been installed on the base.
Package Versions	Lists the individual software modules of the mGuard. Can be used for support purposes.	

4.3.6 Update

Firmware updates with firewall redundancy enabled

Updates of Version 7.3.1 or later can be performed while an mGuard redundant pair is connected and operating.

This does not apply to the following devices:

– mGuard industrial rs
– mGuard smart
– mGuard pci
– mGuard blade
– mGuard delta

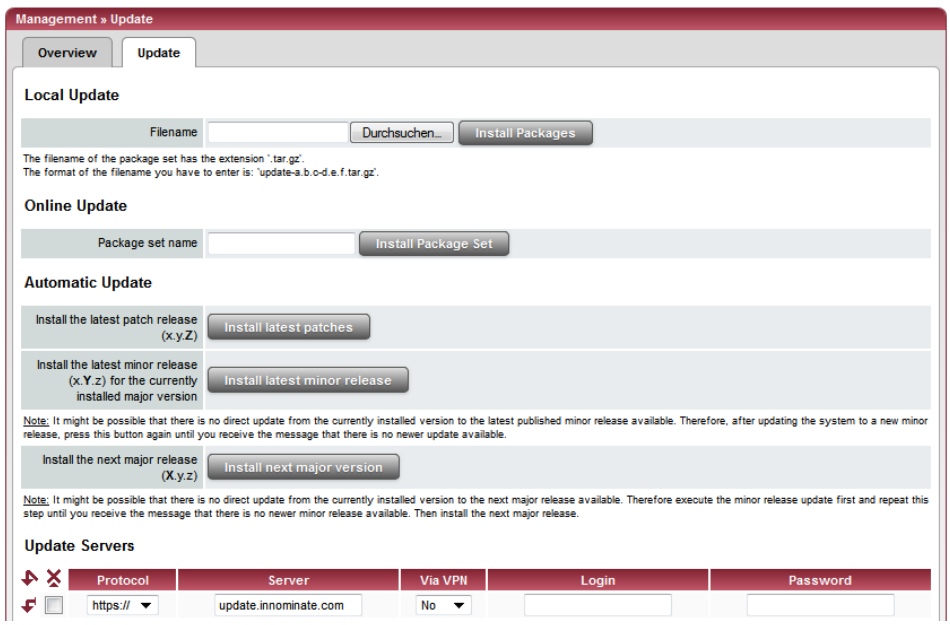
These devices must be updated successively while the relevant redundant device is disconnected.

If firewall redundancy is activated, the two mGuard devices of a redundant pair can be updated at the same time. mGuard devices that form a pair automatically decide which mGuard is to perform the update first while the other mGuard remains active. If the active mGuard is unable to boot within 25 minutes of receiving the update command (because the other mGuard has not yet taken over), it aborts the update and continues to run using the existing firmware version.

Updating the firmware

There are two options for performing a firmware update:

1. You have the current package set file on your computer (the file name ends with ".tar.gz") and you perform a local update.
2. The mGuard downloads a firmware update of your choice from the update server via the Internet and installs it.


Management » Update
Overview
Update
Local Update
Filename
Durchsuchen...
Install Packages
The filename of the package set has the extension '.tar.gz'.
The format of the filename you have to enter is: 'update-a.b.c-d.e.f.tar.gz'.
Online Update
Package set name
Install Package Set
Automatic Update
Install the latest patch release (x.y.Z)
install latest patches
Install the latest minor release (x.Y.z) for the currently installed major version
Install latest minor release
Note: It might be possible that there is no direct update from the currently installed version to the latest published minor release available. Therefore, after updating the system to a new minor release, press this button again until you receive the message that there is no newer update available.
Install the next major release (X.y.z)
install next major version
Note: It might be possible that there is no direct update from the currently installed version to the next major release available. Therefore execute the minor release update first and repeat this step until you receive the message that there is no newer minor release available. Then install the next major release.
Update Servers
Protocol
Server
Via VPN
Login
Password
https://
update.innominate.com
No

NOTE: Do not interrupt the power supply to the mGuard during the update process. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

	Depending on the size of the update, the process may take several minutes.
	A message is displayed if a restart is required after completion of the update.
	With mGuard firmware Version 5.0.0 or later, a license must be obtained for the relevant device before a major release upgrade (e.g., from Version 5.x.y to Version 6.x.y or from Version 6.x.y to Version 7.x.y) can be installed. The license must be installed on the device before updating the firmware (see “Management >> Licensing” on page 67 and “Install” on page 67). Minor release upgrades (i.e., the same major version, e.g., within Version 7.x.y) can be installed without a license until further notice.

Management >> Update		
Local Update	**Filename**	To install the packages, proceed as follows: • Click on **Browse...**, select the file, and open it so that the file name or path is displayed in the *Filename* field. The file name must have the following format: update-a.b.c-d.e.f.default.<platform>.tar.gz **Example**: update-7.0.0-7.0.1.default.ixp4xx_be.tar.gz • Then click on **Install Packages**.
Online Update	**Package set name**	To perform an online update, proceed as follows: • Make sure that there is at least one valid entry under **Update Servers**. You should have received the necessary details from your licenser. • Enter the name of the package set, e.g., “update-6.1.x-7.2.0”. • Then click on **Install Package Set**.
Automatic Update	This is a version of the online update where the mGuard independently determines the required package set.	
	Install the latest patch release (x.y.Z)	Patch releases resolve errors in previous versions and have a version number which only changes in the third digit position. For example, 4.0.1 is a patch release for Version 4.0.0.
	Install the latest minor release (x.Y.z) for the currently installed major version	Minor and major releases supplement the mGuard with new properties or contain changes that affect the behavior of the mGuard. Their version number changes in the first or second digit position.
	Install the next major release (X.y.z)	For example, 4.1.0 is a major or minor release for versions 3.1.0 or 4.0.1 respectively.

Management >> Update [...]

Update Servers

Specify from which servers an update may be performed.

The list of servers is processed from top to bottom until an available server is found. The order of the entries therefore also specifies their priority.

All configured update servers must provide the same updates.

The following options are available:

Protocol The update can be performed via HTTPS or HTTP.

Server Host name of the server that provides the update files.

Via VPN The update is performed via the VPN tunnel.

Default: No.

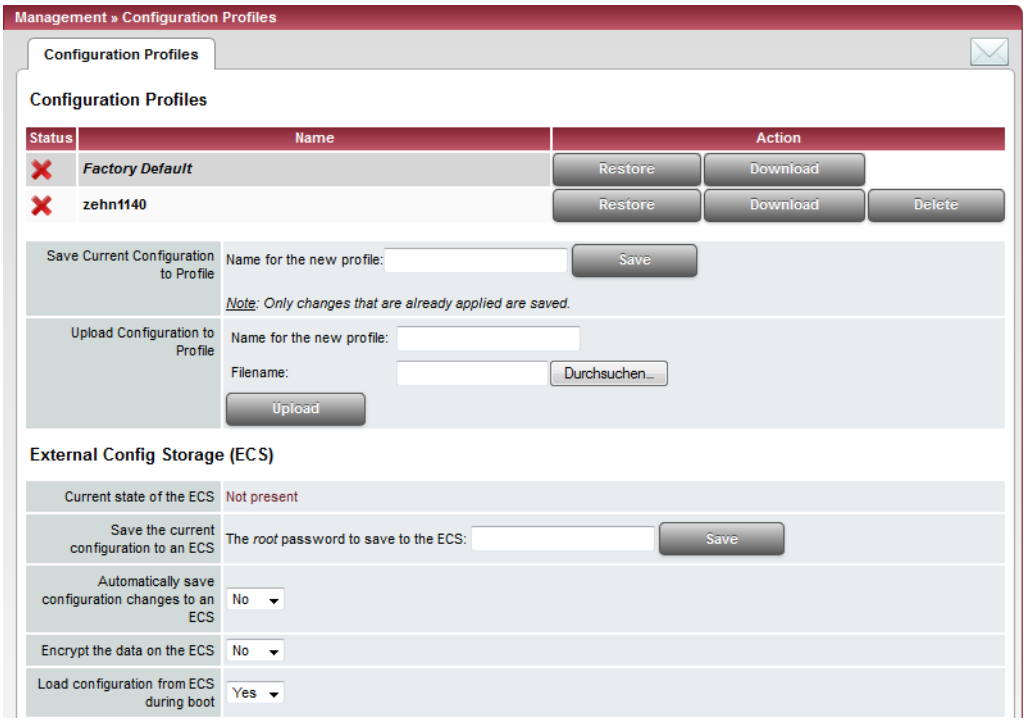
Updates via VPN are not supported if the relevant VPN tunnel has been disabled in the configuration (see *IPsec VPN >> Connections*) and has only been temporarily opened via the service contact or CGI interface.

Login Login for the server.

Password Password for login.

4.4 Management >> Configuration Profiles

4.4.1 Configuration Profiles



You can save the settings of the mGuard as a configuration profile under any name on the mGuard. It is possible to create multiple configuration profiles. You can then switch between different profiles as required, for example, if the mGuard is used in different environments.

Furthermore, you can also save the configuration profiles as files on your configuration computer. Alternatively, these configuration files can be loaded onto the mGuard and activated.

In addition, you can restore the *Factory Default* settings at any time.

Certain models also allow the configuration profiles to be stored on external configuration storage (ECS).

- **SD card:** mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard delta², mGuard pci² SD, mGuard pcie² SD
- **V.24/USB memory stick:** EAGLE mGuard, mGuard centerport

(See “Profiles on an external storage medium” on page 78.)

When a configuration profile is saved, the passwords used for authenticating administrative access to the mGuard are not saved.

It is possible to load and activate a configuration profile that was created under an older firmware version. However, the reverse is not true – a configuration profile created under a newer firmware version should not be loaded and will be rejected.

Encrypted configuration memory

In the case of platform 2 mGuard and firmware 7.6.1 or later, the configuration storage (ECS) and configuration profile (ATV) can be encrypted. This makes the rollout easier. You can save several mGuard configurations on an SD card and then use it to startup all mGuards. During the startup process, the mGuard finds the valid configurations on the SD card. This is loaded, decrypted, and used as a valid configuration (see “Encrypt the data on the ECS” on page 77.)

Management >> Configuration Profiles

Configuration Profiles

At the top of the page there is a list of the configuration profiles that are stored on the mGuard, e.g., the *Factory Default* configuration profile. If any configuration profiles have been saved by the user (see below), they will be listed here.

Active configuration profile: the configuration profile that is currently enabled has an *Active* symbol at the start of the entry.

Configuration profiles that are stored on the mGuard can be:

– Enabled
– Saved as a file on the connected configuration computer
– Deleted
– Displayed

Displaying the configuration profile:

- Click on the name of the configuration profile in the list.

Enabling the factory default or a configuration profile saved on the mGuard **by the user:**

- Click on **Restore** to the right of the name of the relevant configuration profile.
  The corresponding configuration profile is activated.

Saving the configuration profile as a file on the configuration computer:

- Click on **Download** to the right of the name of the relevant configuration profile.
- In the dialog box that is displayed, specify the file name and folder under which the configuration profile is to be saved as a file.
  (The file name can be freely selected.)

Deleting a configuration profile:

- Click on **Delete** to the right of the name of the relevant configuration profile.

The *Factory Default* profile cannot be deleted.

Save Current Configuration to Profile

Saving the active configuration as a configuration profile on the mGuard:

- Enter the desired profile name in the *Name for the new profile* field next to “Save Current Configuration to Profile”.
- Click on **Save**.
  The configuration profile is saved on the mGuard, and the name of the profile appears in the list of profiles already stored on the mGuard.

Management >> Configuration Profiles [...]		
Upload Configuration to Profile	**Uploading a configuration profile that has been saved to a file on the configuration computer:** **Requirement**: a configuration profile has been saved on the configuration computer as a file according to the procedure described above. • Enter the desired profile name in the *Name for the new profile* field next to “Upload Configuration to Profile”. • Click on **Browse...**, select and open the relevant file in the dialog box that is displayed. • Click on **Upload**. The configuration profile is loaded on the mGuard, and the name assigned in step 1 appears in the list of profiles already stored on the mGuard.	
External Config Storage (ECS)	**Current state of the ECS**	The current state is updated dynamically. (See “State of the External Configuration Storage ECS” in “Event table” on page 53).
	Save the current configuration to an ECS	*Only for mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard delta², mGuard pci² SD,* mGuard pcie² SD, *EAGLE mGuard, and mGuard centerport* When replacing the original device with a replacement device, the configuration profile of the original device can be applied using the ECS. To do so, the replacement device must still use “root” as the password for the “root” user. If the root password on the replacement device is not “root”, this password must be entered in the **The root password to save to the ECS** field. (See “Saving a profile to an external storage medium”)
	Automatically save configuration changes to an ECS	*Only for mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard delta², mGuard pci² SD,* mGuard pcie² SD, *EAGLE mGuard, and mGuard centerport* When set to **Yes**, the configuration changes are automatically saved to the ECS, i.e., the ECS always stores the profile currently used. The mGuard only uses the automatically stored configuration profiles upon startup if the original password (“root”) is still set on the mGuard for the “root” user (see “Loading a profile from an external storage medium” on page 78). Configuration changes are also made, if the ECS is disconnected, full, or defective. The corresponding error messages are displayed in the Logging menu (see “Logging >> Browse local logs”). Activation of the new setting extends the response time of the user interface when changing any settings.

Management >> Configuration Profiles [...]		
	Encrypt the data on the ECS	*Only for mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard pci² SD,* mGuard pcie² SD*, mGuard delta², mGuard centerport* In the case of firmware 7.6.1 or later, the configuration storage (ECS) and configuration profile (ATV) can be encrypted. This makes the mGuard rollout easier. You can save several mGuard configurations on an SD card (on a USB stick in the case of mGuard centerport) and then use it to startup all mGuards. During the startup process, the mGuard finds the valid configurations on the configuration storage. This is loaded, decrypted, and used as a valid configuration. If **Yes** is selected, the configuration changes are encrypted and stored on an ECS.
	Load configuration from ECS during boot	When set to **Yes**, the ECS is accessed during the boot process.

Profiles on an external storage medium

mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard delta², mGuard pci² SD, mGuard pcie² SD, EAGLE mGuard, mGuard centerport

EAGLE mGuard: the configuration profiles can also be stored on external configuration storage (ECS).

mGuard centerport and **EAGLE mGuard** with **USB interface**: the configuration profiles can also be stored on a USB stick. This must have the following properties:

– FAT file system on the first primary partition, at least 64 Mbytes free memory capacity.

mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard delta², mGuard pci² SD, mGuard pcie² SD: configuration profiles can also be stored on an SD card (up to 2 GB capacity). It must have the following properties:

– FAT file system on the first primary partition, at least 64 Mbytes free memory capacity.
– Certified and released by Innominate Security Technologies AG (current release list can be found at www.innominate.com).

Saving a profile to an external storage medium

- **EAGLE mGuard**: connect the ECS to the V.24 socket (ACA11) or USB socket (ACA21). Type ACA21 ECS devices are not suitable for manual modifications by a computer or similar.
- **mGuard centerport and EAGLE mGuard** and **with USB interface**: insert the USB stick into the USB socket.
- **mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard delta², mGuard pci² SD, mGuard pcie² SD**: insert the SD card into the SD slot at the front.
- If the root password on the mGuard onto which the profile is going to be subsequently loaded is not “root”, this password must be entered in the **The root password to save to the ECS** field.
- Click on **Save**.

  For EAGLE mGuard: the LED STATUS and LED V.24 flash until the saving process is complete.

Loading a profile from an external storage medium

- **EAGLE mGuard**: connect the ECS to the V.24 socket (ACA11) or USB socket (ACA21). Type ACA21 ECS are not suitable for manual modifications by a computer or similar.
- **mGuard centerport** and **EAGLE mGuard with USB interface**: insert the USB stick into the USB socket.
- **mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard delta², mGuard pci² SD, mGuard pcie² SD**: insert the SD card into the SD slot at the front.
- Once the storage medium has been inserted, start the mGuard.
- The mGuard root password must either be “root” or correspond to the password that was specified while the profile was being saved.

  For EAGLE mGuard: the LED STATUS and LED V.24 flash until the saving process is complete.

The configuration profile loaded from the storage medium is loaded onto the mGuard and applied.

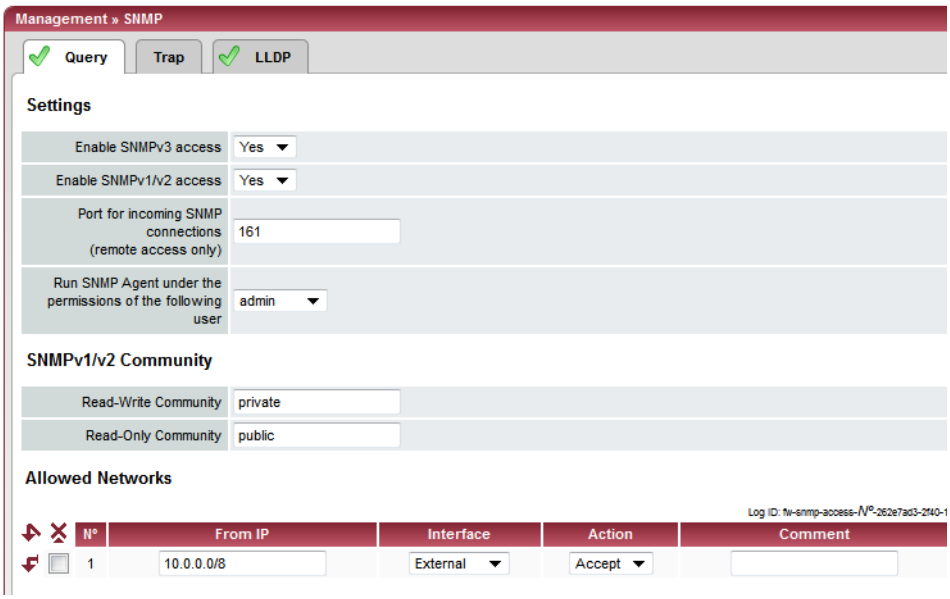
The loaded configuration profile does not appear in the list of configuration profiles stored on the mGuard.

The configuration on the external storage medium also contains the passwords for the *root*, *admin*, *netadmin*, *audit*, and *user* users. These passwords are also loaded when loading from an external storage medium. The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager.

4.5 Management >> SNMP

The mGuard must not be simultaneously configured via the web access, shell access, or SNMP. Simultaneous configuration via the different access methods might lead to unexpected results.

4.5.1 Query



The SNMP (Simple Network Management Protocol) is mainly used in more complex networks to monitor the state and operation of devices.

SNMP is available in several releases: SNMPv1/SNMPv2 and SNMPv3.

The older versions (SNMPv1/SNMPv2) do not use encryption and are not considered to be secure. The use of SNMPv1/SNMPv2 is therefore not recommended.

SNMPv3 is significantly better in terms of security, but not all management consoles support this version yet.

If SNMPv3 or SNMPv1/v2 is activated, this is indicated by a green signal field on the tab at the top of the page. Otherwise, i.e., if SNMPv3 or SNMPv1/v2 is not active, the signal field is red.

Processing an SNMP request may take more than one second. However, this value corresponds to the default timeout value of some SNMP management applications.

- If you experience timeout problems, set the timeout value of your management application to values between 3 and 5 seconds.

Management >> SNMP >> Query		
Settings	**Enable SNMPv3 access: Yes/No**	If you wish to allow monitoring of the mGuard via SNMPv3, set this option to **Yes**. The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access and monitoring options on the mGuard. Access via SNMPv3 requires authentication with a login and password. The default settings for the login parameters are: **Login**: admin **Password**: SnmpAdmin (please note that the password is case-sensitive) MD5 is supported for the authentication process; DES is supported for encryption. The login parameters for SNMPv3 can only be changed using SNMPv3.
	Enable SNMPv1/v2 access: Yes/No	If you wish to allow monitoring of the mGuard via SNMPv1/v2, set this option to **Yes**. You must also enter the login data under **SNMPv1/v2 Community**. The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access and monitoring options on the mGuard.
	Port for incoming SNMP connections	Default: 161 If this port number is changed, the new port number only applies for access via the *External, External 2, VPN*, and *Dial-in* interface. Port number 161 still applies for internal access. The remote partner that implements remote access may have to specify the port number defined here during entry of the address.
SNMPv1/v2 Community	**Read-Write Community**	Enter the required login data in this field.
	Read-Only Community	Enter the required login data in this field.

Management >> SNMP >> Query [...]

Allowed Networks

Lists the firewall rules that have been set up. These apply for incoming data packets of an SNMP access attempt.

The rules specified here only take effect if **Enable SNMPv3 access** or **Enable SNMPv1/v2 access** is set to **Yes**.

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

From IP

Enter the address of the computer or network from which remote access is permitted or forbidden in this field.

The following options are available:

– An IP address.
– To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).
– **0.0.0.0/0** means all addresses.

Interface

External/Internal/External 2/VPN/Dial-in[1]

Specifies to which interface the rule should apply.

If no rules are set or if no rule applies, the following default settings apply:

SNMP monitoring is permitted via *Internal, VPN*, and *Dial-in*.

Access via *External* and *External 2* is refused.

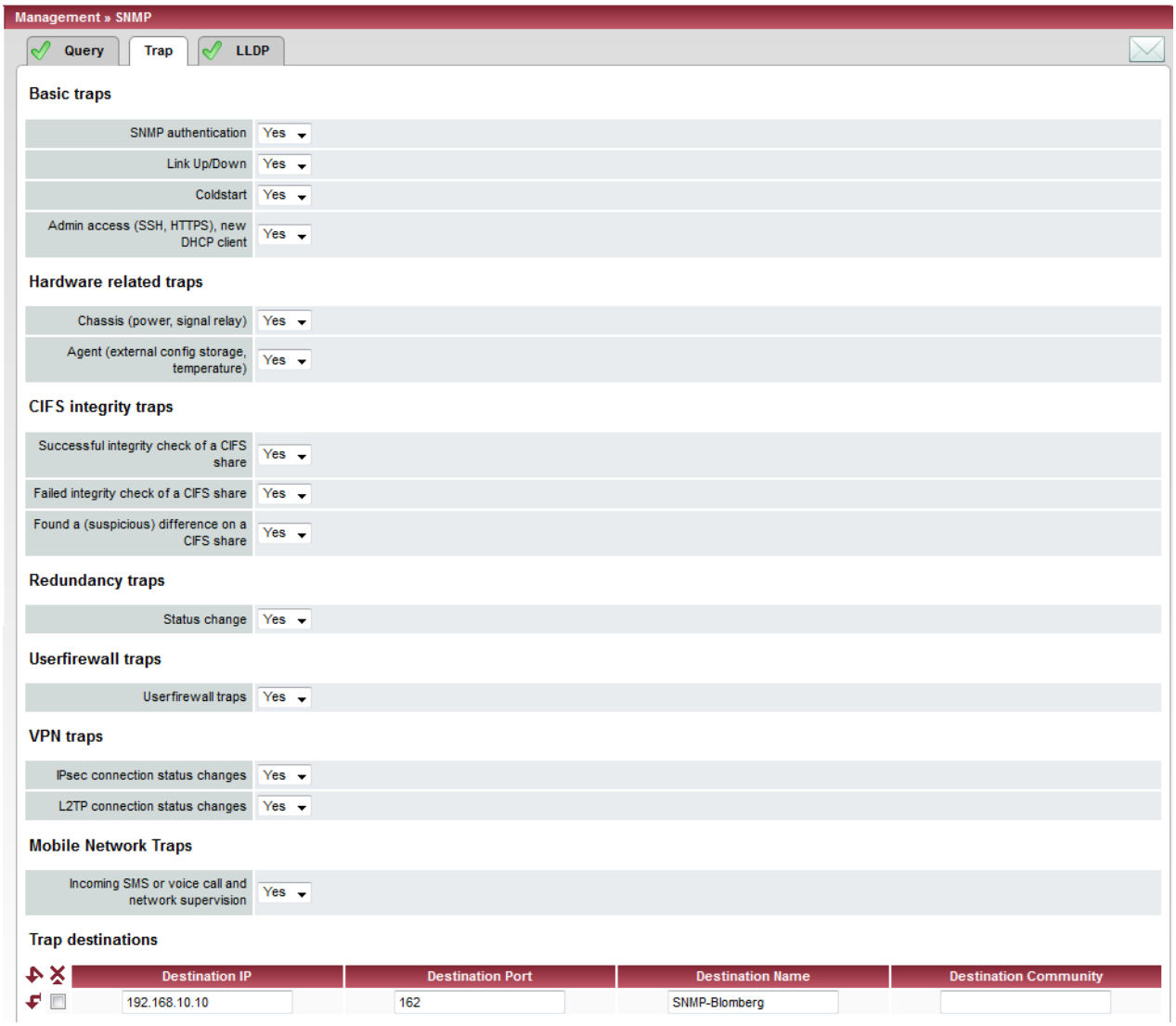
Specify the monitoring options according to your requirements.

NOTE: If you want to refuse access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as an action. **To prevent your own access being blocked**, you may have to permit access simultaneously via another interface explicitly with *Accept* before clicking on the **Apply** button to activate the new setting. Otherwise, if your access is blocked, you must carry out the recovery procedure.

Management >> SNMP >> Query [...]		
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.) **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default setting)

[1] *External 2* and *Dial-in* are only for devices with a serial interface (see “Network >> Interfaces” on page 105).

4.5.2 Trap



In certain cases, the mGuard can send SNMP traps. SNMP traps are only sent if the SNMP request is activated.

The traps correspond to SNMPv1. The trap information for each setting is listed below. A more detailed description can be found in the MIB that belongs to the mGuard.

If SNMP traps are sent to the partner via a VPN channel, the IP address of the partner must be located in the network that is specified as the **Remote** network in the definition of the VPN connection.

The internal IP address must be located in the network that is specified as **Local** in the definition of the VPN connection (see IPsec VPN >> Connections >> Edit >> General).

– If the IPsec VPN >> Connections >> Edit >> General, **Local** option is set to **1:1 NAT** (see Page 263), the following applies:

  The internal IP address must be located in the specified local network.

– If the IPsec VPN >> Connections >> Edit >> General, **Remote** option is set to **1:1 NAT** (see Page 265), the following applies:

  The IP address of the SysLog server must be located in the network that is specified as **Remote** in the definition of the VPN connection.

Management >> SNMP >> Trap		
Basic traps	**SNMP authentication**	Activate traps **Yes/No** – enterprise-oid : mGuardInfo – generic-trap : authenticationFailure – specific-trap : 0 Sent if an unauthorized station attempts to access the mGuard SNMP agent.
	Link Up/Down	Activate traps **Yes/No** – enterprise-oid : mGuardInfo – generic-trap : linkUp, linkDown – specific-trap : 0 Sent when the connection to a port is interrupted (linkDown) or restored (linkUp).
	Coldstart	Activate traps **Yes/No** – enterprise-oid : mGuardInfo – generic-trap : coldStart – specific-trap : 0 Sent after a cold restart or warm start.
	Admin access (SSH, HTTPS), new DHCP client	Activate traps **Yes/No** – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardHTTPSLoginTrap (1) – additional : mGuardHTTPSLastAccessIP This trap is sent if someone has tried successfully or unsuccessfully (e.g., using an incorrect password) to open an HTTPS session. The trap contains the IP address from which the attempt was issued. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardShellLoginTrap (2) – additional : mGuardShellLastAccessIP This trap is sent when someone opens the shell via SSH or the serial interface. The trap contains the IP address of the login request. If this request was sent via the serial interface, the value is 0.0.0.0.

Management >> SNMP >> Trap [...]		
		– enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : 3 – additional : mGuardDHCPLastAccessMAC This trap is sent when a DHCP request is received from an unknown client. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSSHLogin – additional : mGuardTResSSHUsername mGuardTResSSHRemoteIP This trap is sent when someone accesses the mGuard via SSH. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSSHLogout – additional : mGuardTResSSHUsername mGuardTResSSHRemoteIP This trap is sent when access to the mGuard via SSH is terminated.
Hardware related traps (only mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard industrial rs, EAGLE mGuard)	**Chassis (power, signal relay)**	Activate traps **Yes/No** – enterprise-oid : mGuardTrapSenderIndustrial – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapIndustrialPowerStatus (2) – additional : mGuardTrapIndustrialPowerStatus Sent when the system registers a power failure. – enterprise-oid : mGuardTrapSenderIndustrial – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSignalRelais (3) – additional : mGuardTResSignalRelaisState (mGuardTEsSignlalRelaisReason, mGuardTResSignal RelaisReasonIdx) Sent after the signal contact is changed and indicates the current status (0 = Off, 1 = On).

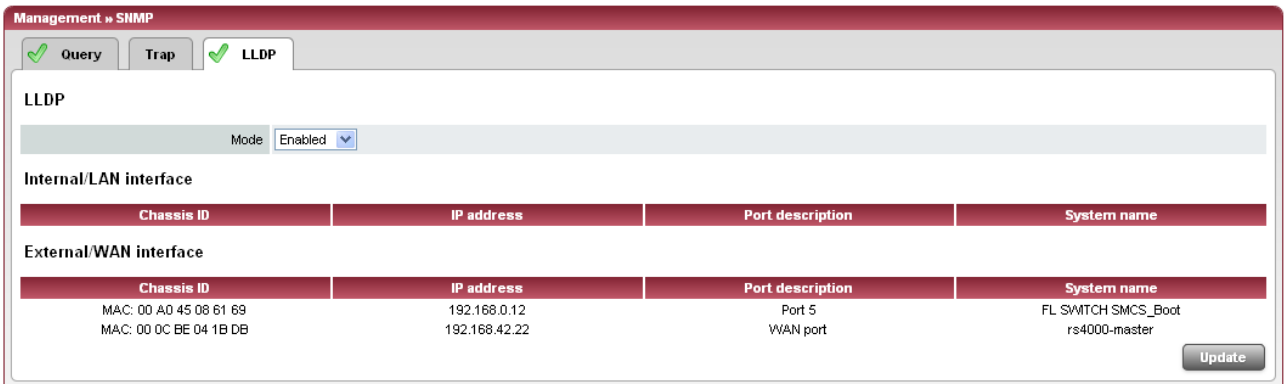
Management >> SNMP >> Trap [...]		
	Agent (external config storage, temperature)	Activate traps **Yes/No** – enterprise-oid : mGuardTrapIndustrial – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapIndustrialTemperature (1) – additional : mGuardSystemTemperature, mGuardTrapIndustrialTempHiLimit, mGuardTrapIndustrialLowLimit The trap indicates the temperature in the event of the temperature exceeding the specified limit values. – enterprise-oid : mGuardTrapIndustrial – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapAutoConfigAdapterState (4) – additional : mGuardTrapAutoConfigAdapter Change This trap is sent after access to the ECS.
mGuard blade Controller traps (BLADE only)	**Blade status change**	(Blade switch, failure): activate traps **Yes/No** – enterprise-oid : mGuardTrapBladeCTRL – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlPowerStatus (2) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlPowerStatus This trap is sent when the power supply status of the blade pack changes. – enterprise-oid : mGuardTrapBladeCTRL – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlRunStatus (3) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlRunStatus This trap is sent when the blade run status changes.
	Blade reconfiguration	(Backup/restore): activate traps **Yes/No** – enterprise-oid : mGuardTrapBladeCtrlCfg – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlCfgBackup (1) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlCfgBackup This trap is sent when configuration backup is triggered for the mGuard blade controller.

Management >> SNMP >> Trap [...]		
		– enterprise-oid : mGuardTrapBladeCtrlCfg – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlCfgRestored 2 – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlCfgRestored This trap is sent when configuration restoration is triggered from the mGuard blade controller.
CIFS integrity traps This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.	**Successful integrity check of a CIFS share**	Activate traps **Yes/No** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanInfo (1) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs This trap is sent if the CIFS integrity check has been successfully completed.
	Failed integrity check of a CIFS share	Activate traps **Yes/No** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanFailure (2) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs This trap is sent if the CIFS integrity check has failed.
	Found a (suspicious) difference on a CIFS share	Activate traps **Yes/No** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanDetection (3) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs This trap is sent if the CIFS integrity check has detected a deviation.
Userfirewall traps This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.	**Userfirewall traps**	Activate traps **Yes/No** – enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallLogin (1) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthenticationMethod This trap is sent when a user logs into the user firewall.

Management >> SNMP >> Trap [...]		
		– enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallLogout (2) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallLogoutReason This trap is sent when a user logs out of the user firewall. – enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallAuthError TRAP-TYPE (3) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthentication-Method This trap is sent in the event of an authentication error.
VPN traps	**IPsec connection status changes**	Activate traps **Yes/No** – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNIKEServerStatus (1) – additional : mGuardTResVPNStatus This trap is sent when the IPsec IKE server is started or stopped. – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNIPsecConnStatus (2) – additional : mGuardTResVPNName, mGuardTResVPNIndex, mGuardTResVPNPeer, mGuardTResVPNStatus, mGuardTResVPNType, mGuardTResVPNLocal, mGuardTResVPNRemote This trap is sent when the status of an IPsec connection changes. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapVPNIPsecConnStatus This trap is sent when a connection is established or aborted. It is not sent when the mGuard is about to accept a connection request for this connection.

Management >> SNMP >> Trap [...]		
	L2TP connection status changes	Activate traps **Yes/No** – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNL2TPConnStatus (3) – additional : mGuardTResVPNName, mGuardTResVPNIndex, mGuardTResVPNPeer, mGuardTResVPNStatus, mGuardTResVPNLocal, mGuardTResVPNRemote This trap is sent when the status of an L2TP connection changes.
Mobile network traps This menu item is only included in the scope of functions for the mGuard rs4000 3G, mGuard rs2000 3G.	**Incoming text message or voice call and network supervision**	Enables traps for mobile phone connection. Traps are sent when an text message is received, a call is received or the mobile phone connection drops.
Trap destinations	**Traps can be sent to multiple destinations.**	
	Destination IP	IP address to which the trap should be sent.
	Destination Port	Default: 162 Destination port to which the trap should be sent.
	Destination Name	Optional name for the destination. Does not affect the generated traps.
	Destination Community	Name of the SNMP community to which the trap is assigned.

4.5.3 LLDP

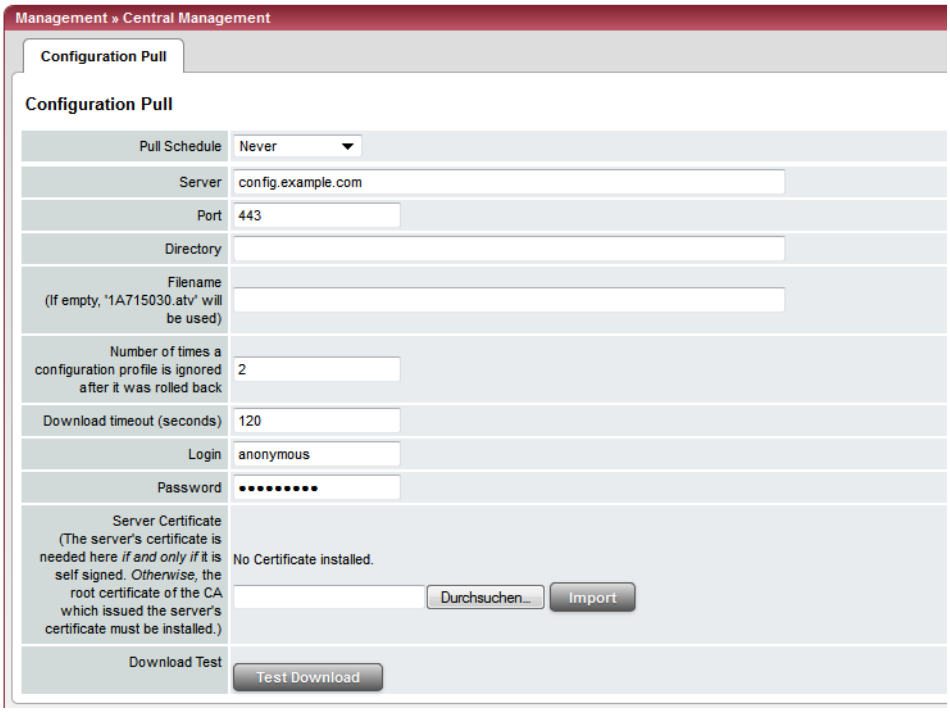


LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) uses suitable request methods to automatically determine the (Ethernet) network infrastructure. LLDP-capable devices periodically send Ethernet multicasts (layer 2). Tables of systems connected to the network are created from the responses, and these can be requested via SNMP.

Management >> SNMP >> LLDP		
LLDP	**Mode**	**Enabled/Disabled** The LLDP service or agent can be globally enabled or disabled here. If the function is enabled, this is indicated by a green signal field on the tab at the top of the page. If the signal field is red, the function is disabled.
Internal/LAN interface **External/WAN interface**	**Chassis ID**	A unique ID of the computer found; typically one of its MAC addresses.
	IP address	IP address of the computer found. This can be used to perform administrative activities on the computer via SNMP.
	Port description	A textual description of the network interface where the computer was found.
	System name	Host name of the computer found.
	Button: Update	To update the displayed data, if necessary, click on **Update**.

4.6 Management >> Central Management

4.6.1 Configuration Pull



The mGuard can retrieve new configuration profiles from an HTTPS server in adjustable time intervals, provided that the server makes them available to the mGuard as files (file extension: .atv). If the configuration provided differs from the active configuration of the mGuard, the available configuration is automatically downloaded and activated.

Management >> Central Management >> Configuration Pull		
Configuration Pull	**Pull Schedule**	Here, specify whether (and if so, when and at what intervals) the mGuard should attempt to download and apply a new configuration from the server. To do this, open the selection list and select the desired value. A new field is shown when **Time Schedule** is selected. In this field, specify whether the new configuration should be downloaded from the server daily or regularly on a certain weekday, and at what time. Time-controlled download of a new configuration is only possible if the system time has been synchronized (see “Management >> System Settings” on page 33, “Time and Date” on page 35). Time control sets the selected time based on the configured time zone.
	Server	IP address or host name of the server that provides the configurations.

Management >> Central Management >> Configuration Pull [...]

Directory	The directory (folder) on the server where the configuration is located.
Filename	The name of the file in the directory defined above. If no file name is defined here, the serial number of the mGuard is used with file extension ".atv".
Number of times a configuration profile is ignored after it was rolled back	Default: 10 After retrieving a new configuration, it is possible that the mGuard may no longer be accessible after applying the new configuration. It is then no longer possible to implement a new remote configuration to make corrections. In order to prevent this, the mGuard performs the following check:

As soon as the retrieved configuration is applied, the mGuard tries to connect to the configuration server again based on the new configuration. It then attempts to download the newly applied configuration profile again.

If successful, the new configuration remains in effect.

If this check is unsuccessful for whatever reason, the mGuard assumes that the newly applied configuration profile is faulty. The mGuard remembers the MD5 total for identification purposes. The mGuard then performs a rollback.

Rollback means that the last (working) configuration is restored. This assumes that the new (non-functioning) configuration contains an instruction to perform a rollback if a newly loaded configuration profile is found to be faulty according to the checking procedure described above.

When the mGuard makes subsequent attempts to retrieve a new configuration profile periodically after the time defined in the **Pull Schedule** field (and **Time Schedule**) has elapsed, it will only accept the profile subject to the following selection criterion: the configuration profile provided **must differ** from the configuration profile previously identified as faulty for the mGuard and which resulted in the rollback.

(The mGuard checks the MD5 total stored for the old, faulty, and rejected configuration against the MD5 total of the new configuration profile offered.)

If this selection criterion is **met**, i.e., a newer configuration profile is offered, the mGuard retrieves this configuration profile, applies it, and checks it according to the procedure described above. It also disables the configuration profile by means of rollback if the check is unsuccessful.

If the selection criterion is **not met** (i.e., the same configuration profile is being offered), the selection criterion remains in force for all further cyclic requests for the period specified in the **Number of times...** field.

If the specified number of times elapses without a change of the configuration profile on the configuration server, the mGuard applies the unchanged new ("faulty") configuration profile again, despite it being "faulty". This is to rule out the possibility that external factors (e.g., network failure) may have resulted in the check being unsuccessful.

The mGuard then attempts to connect to the configuration server again based on the new configuration that has been reapplied. It then attempts to download the newly applied configuration profile again. If this is unsuccessful, another rollback is performed. The selection criterion is enforced again for the further cycles for loading a new configuration as often as is defined in the **Number of times...** field.

Management >> Central Management >> Configuration Pull [...]

If the value in the **Number of times...** field is specified as **0**, the selection criterion (the offered configuration profile is ignored if it remains unchanged) will never be enforced. As a result, the second of the following objectives could then no longer be met.

This mechanism has the following objectives:

1. After applying a new configuration, it must be ensured that the mGuard can still be configured from a remote location.
2. When cycles are close together (e.g., **Pull Schedule** = 15 minutes), the mGuardMGUARD must be prevented from repeatedly testing a configuration profile that might be faulty at intervals that are too short. This can hinder or prevent external administrative access, as the mGuard might be too busy dealing with its own processes.
3. External factors (e.g., network failure) must be largely ruled out as a reason why the mGuard considers the new configuration to be faulty.

Download timeout (seconds)	Default: 120. Specifies the maximum timeout length (period of inactivity) when downloading the configuration file. The download is aborted if this time is exceeded. If and when a new download is attempted depends on the setting of *Pull Schedule* (see above).
Login	Login (user name) that the HTTPS server requests.
Password	Password that the HTTPS server requests.
Server Certificate	The certificate that the mGuard uses to check the authenticity of the certificate “shown” by the configuration server. It prevents an incorrect configuration from an unauthorized server from being installed on the mGuard. The following may be specified here: – A self-signed certificate of the configuration server or – The root certificate of the CA (certification authority) that issued the server certificate. This is valid when the configuration server certificate is signed by a CA (instead of self-signed).

Management >> Central Management >> Configuration Pull [...]

If the stored configuration profiles also contain the private VPN key for the VPN connection(s) with PSK, the following conditions must be met:

– The password should consist of at least 30 random upper and lower case letters and numbers (to prevent unauthorized access).
– The HTTPS server should only grant access to the configuration of this individual mGuard using the login and password specified. Otherwise, users of other mGuard devices could access this individual device.

The IP address or the host name specified under Server must be the same as the server certificate's common name (CN).

Self-signed certificates should not use the “key-usage” extension.

To install a certificate, proceed as follows:

Requirement: the certificate file must be saved on the connected computer.

- Click on **Browse...** to select the file.
- Click on **Import**.

Download Test

- By clicking on **Test Download**, you can test whether the specified parameters are correct without actually saving the modified parameters or activating the configuration profile. The result of the test is displayed in the right-hand column.

Ensure that the profile on the server does not contain unwanted variables starting with “GAI_PULL_”, as these overwrite the applied configuration.

4.7 Management >> Service I/O

This menu is **only** available on the **mGuard rs4000/rs2000 3G**, **mGuard rs4000/rs2000**, **mGuard industrial rs**.

Service contacts (service I/Os) can be connected to some mGuards.

- **mGuard rs4000/rs2000 3G**
- **mGuard rs4000/rs2000**
- **mGuard industrial rs**

Connection of the service contacts is described in the user manual for the devices (UM EN MGUARD DEVICES).

Input/CMD 1, CMD 2, CMD 3

A push button or an on/off switch can be connected to the inputs. One or more freely selectable VPN connections or firewall rule records can be switched via the corresponding switch. A mixture of VPN connections and firewall rule records is also possible. The web interface displays which VPN connections and which firewall rule records are connected to this input.

The push button or on/off switch is used to establish and release predefined VPN connections or to activate defined firewall rule records.

Signal contact (signal output) ACK 1, 2

You can set whether to monitor specific VPN connections or firewall rule records and to display them using LEDs.

If VPN connections are being monitored, an illuminated LED indicates that VPN connections are established.

Alarm output ACK 3

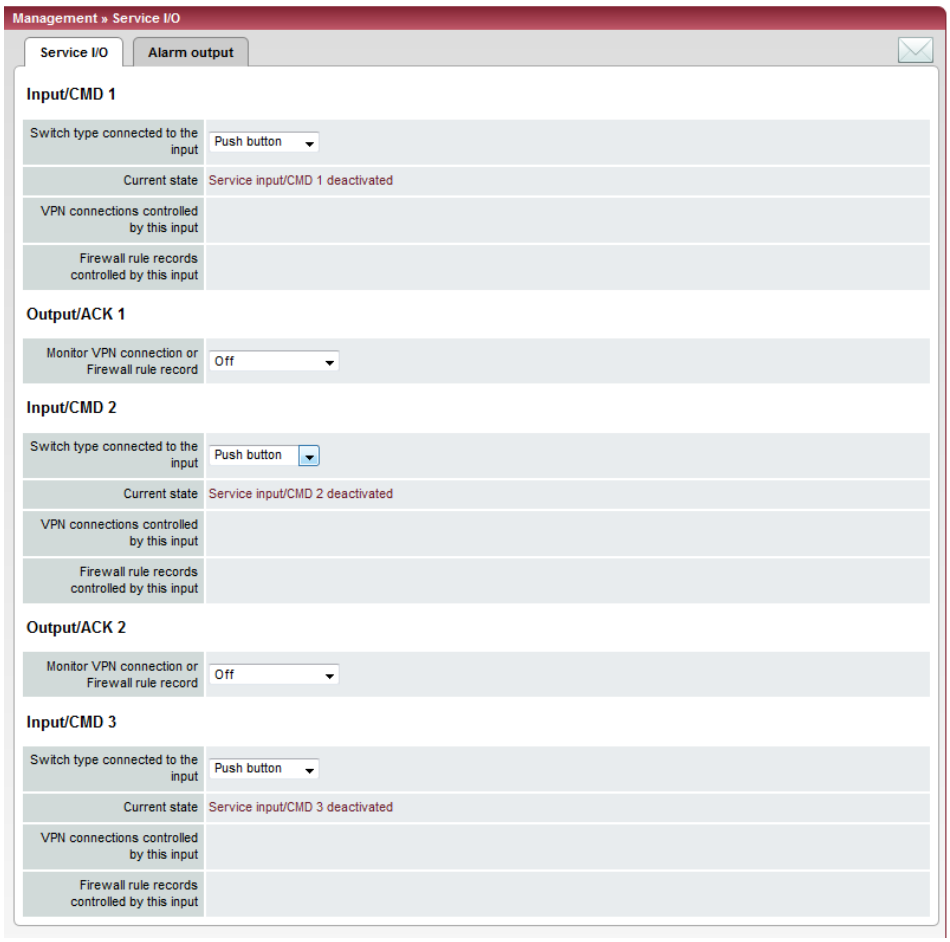
The alarm output monitors the function of the mGuard and therefore enables remote diagnostics.

The associated LED lights up red if the alarm output is open due to an error.

The alarm output reports the following, if it has been activated.

- Failure of the redundant supply voltage
- Monitoring of the link status of the Ethernet connections
- Monitoring of the temperature condition
- Monitoring of the connection state of the internal modem

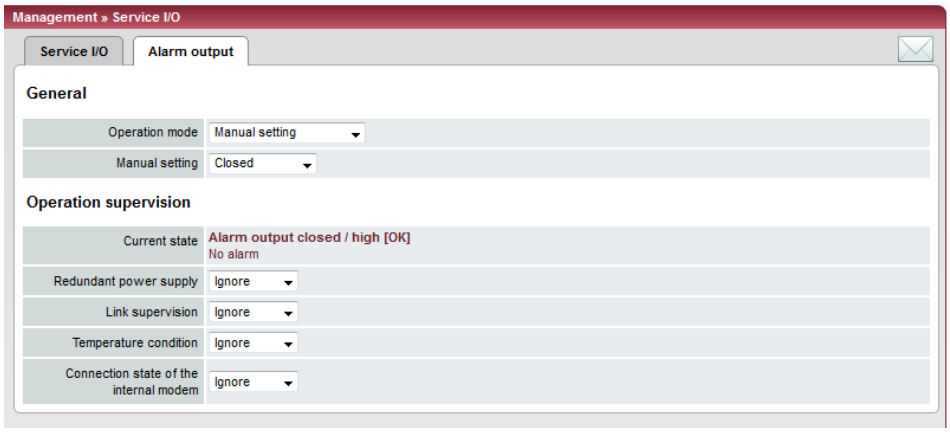
4.7.1 Service I/O



Management >> Service I/O >> Service I/O		
Input/CMD 1-3	**Switch type connected to the input**	**Push button or on/off switch** Select the type of switch connected.
	Current state	Displays the state of the connected switch. When editing the VPN connection, the switch must be selected under “Controlling service input” (under *IPsec VPN* >> *Connections* >> *Edit* >> *General*).

Management >> Service I/O >> Service I/O [...]		
	VPN connections controlled by this input	The mGuard rs4000/rs2000 (3G) and the mGuard industrial rs devices have connections to which external buttons or an on/off switch and actuators (e.g., a signal lamp) can be connected. One of the configured VPN connections can be established and disconnected via the button or on/off switch. The VPN connection is specified here. The display shows the VPN connections that have been set up under *IPsec VPN >> Connections >> Edit >> General*. For the input to be active, the service input must be selected under *Controlling service input* in the *IPsec VPN >> Connections >> Edit >> General* menu.
	Firewall rule records controlled by this input	The display shows the firewall rule records that have been set up under *Network Security >> Packet Filter >> Rule Records*.
Output/ACK 1-2	**Monitor VPN connections or Firewall rule record**	**Off/VPN connections/Rule Records** The state of the selected VPN connection or the selected firewall rule record is indicated via the associated signal contact (ACK output).

4.7.2 Alarm output

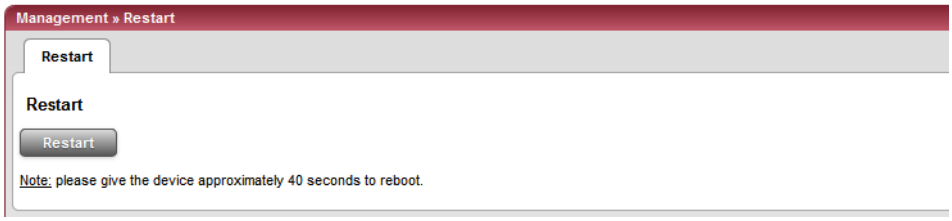


Management >> Service I/O >> Alarm output		
General	**Operation mode**	**Operation supervision/Manual setting** The alarm output can be controlled automatically using **Operation supervision** (default) or **Manual setting**.
	Manual setting	**Closed/Open (Alarm)** The desired state of the alarm output (for function control) can be selected here.
Operation supervision	**Current state**	Displays the state of the alarm output.
	Redundant power supply	Only available with the mGuard rs4000 or mGuard rs4000 3G. If set to **Ignore**, the state of the power supply does not influence the alarm output. If set to **Supervise**, the alarm output is opened if one of the two supply voltages fails.
	Link supervision	**Ignore/Supervise** Monitoring of the link status of the Ethernet connections. If set to **Ignore**, the link status of the Ethernet connections does not influence the alarm output. If set to **Supervise**, the alarm output is opened if one link does not indicate connectivity. Set the links to be monitored under *"Link supervision"* in the *Network >> Ethernet >> MAU settings* menu.
	Temperature condition	The alarm output indicates overtemperature and undertemperature. The permissible range is set under *"System Temperature (°C)"* in the *Management >> System Settings >> Host* menu. If set to **Ignore**, the temperature does not influence the signal contact. If set to **Supervise**, the alarm output is opened if the temperature is not within the permissible range.

Management >> Service I/O >> Alarm output [...]		
	Connection state of the internal modem	Only if an internal modem is available and switched on (mGuard rs4000/rs2000 3G, mGuard industrial rs with internal analog modem or ISDN modem). If set to **Ignore**, the connection status of the internal modem does not influence the alarm output. If set to **Supervise**, the alarm output is opened if the internal modem does not have a connection.
	Connectivity state of redundancy	Only if the “Redundancy” function is used (see Section 16). If set to **Ignore**, the connectivity check does not influence the alarm output. If set to **Supervise**, the alarm output is opened if the connectivity check fails. This is regardless of whether the mGuard is active or in standby mode.

4.8 Management >> Restart

4.8.1 Restart



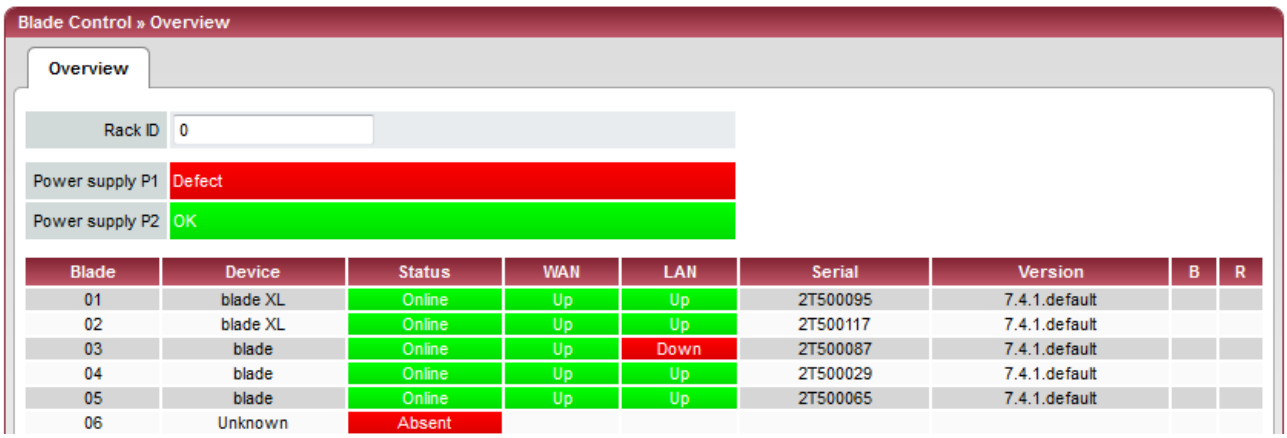
Restarts the mGuard. Has the same effect as a temporary interruption in the power supply, whereby the mGuard is switched off and on again.

A restart (reboot) is necessary in the event of an error. It may also be necessary after a software update.

5 Blade Control menu

This menu is only available on the **mGuard blade controller**. For reasons of compatibility, always use the latest blade slide-in module as controller.

5.1 Blade Control >> Overview

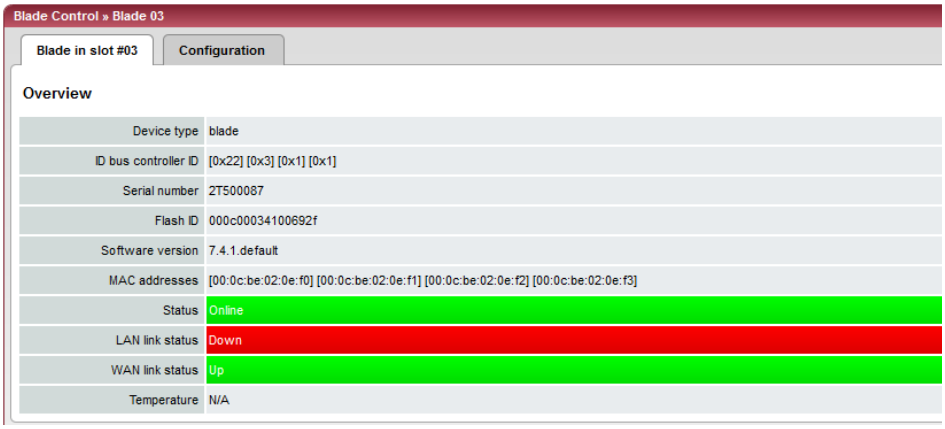


Blade Control >> Overview		
Overview	**Rack ID**	The ID of the rack where the mGuard is located. This value can be configured for all blade devices on the controller.
	Power supply P1/P2	Status of power supply units P1 and P2. – OK – Absent – Defect – Fatal error
	Blade	Number of the slot where the mGuard blade is installed.
	Device	Device name, e.g., “blade” or “blade XL”.
	Status	– **Online -** The device in the slot is operating correctly. – **Present -** The device is present, but not yet ready, e.g., because it is just starting up. – **Absent -** No device found in the slot.
	WAN	Status of the WAN port.
	LAN	Status of the LAN port.
	Serial	Serial number of the mGuard.
	Version	Software version of the mGuard.
	B	**Backup**: automatic configuration backup on the controller is activated/deactivated for this slot.
	R	**Restore**: automatic configuration restoration after replacing the mGuard is activated/deactivated for this slot.

5.2 Blade Control >> Blade 01 to 12

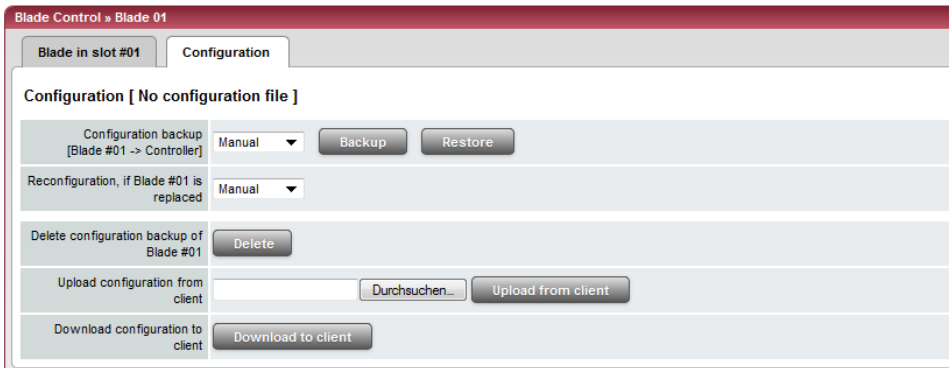
These pages display the status information for each installed mGuard device and enable the configuration of the relevant mGuard device to be backed up and restored.

5.2.1 Blade in slot #...



Blade Control >> Blade xx >> Blade in slot xx		
Overview	**Device type**	Device name, e.g., “blade” or “blade XL”.
	ID bus controller ID	ID of this slot on the control bus of the bladebase.
	Serial number	Serial number of the mGuard.
	Flash ID	Flash ID of the flash memory of the mGuard.
	Software version	Version of the software installed on the mGuard.
	MAC addresses	All MAC addresses used by the mGuard.
	Status	mGuard status.
	LAN status	Status of the LAN port.
	WAN link status	Status of the WAN port.
	Temperature	N/A = Not available

5.2.2 Configuration



Blade Control >> Blade xx >> Configuration		
Configuration The status of the stored configuration is displayed for each blade: **[No configuration file]** **[Out of date]** **[Up to date]** **[File copy in progress]** **[Blade change detected]** **[---]** No blade available **[Configuration upload to Blade[%d] initiated/Configuration upload to Blade[%d] failed.]** **[Configuration download from Blade[%d] initiated/Configuration download from Blade[%d] failed.]** **[Configuration file from Blade[%d] not found]** **[New configuration file for Blade[%d] saved.]** **[Configuration file deletion of Blade[%d] failed.]** **[Configuration file of Blade[%d] deleted.]**	**Configuration backup [Blade #__ -> Controller]**	– **Automatic**: the new configuration is stored automatically on the controller shortly after a configuration change on the mGuard. – **Manual**: the configuration can be stored on the controller by clicking on **Backup**. – Click on **Restore** to transfer the configuration stored on the controller to the mGuard. If the blade was reconfigured after a manual configuration backup, but the new configuration was not saved, the configuration stored on the controller is out of date. This is indicated on the *Configuration* tab page by “Configuration [Obsolete]”. This indicates that something has been overlooked: in this case, you must backup the configuration on the controller.
	Reconfiguration, if mGuard blade is replaced	After replacing an mGuard in this slot, the configuration stored on the controller is automatically transferred to the new device in this slot.
	Delete configuration backup of Blade #__	Deletes the configuration stored on the controller for the device in this slot.
	Upload configuration from client	Uploads and saves the configuration profile for this slot on the controller.
	Download configuration to client	Downloads the configuration profile stored on the controller for this slot onto the configuration PC.

6 Network menu

6.1 Network >> Interfaces

The mGuard has the following interfaces with external access:

	Ethernet: internal: LAN external: WAN	Serial interface	Built-in modem	Serial console via USB[1]
mGuard smart	**Yes**	**No**	**No**	**No**
mGuard smart[2]	**Yes**	**No**	**No**	**Yes**
mGuard rs4000 3G	**LAN: 4 WAN: 1 DMZ: 1**	**Yes**	**Yes**	**No**
mGuard rs2000 3G	**LAN: 4 WAN: no DMZ: no**	**Yes**	**Yes**	**No**
mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs, mGuard pci, mGuard blade, mGuard delta, mGuard delta[2], EAGLE mGuard	**Yes**	**Yes**	**No**	**No**
mGuard pci[2] SD, mGuard pcie[2] SD	**Yes**	**No**	**No**	**No**
Optional: mGuard industrial rs	**Yes**	**Yes**	**Yes**	**No**

[1] See “Serial console via USB” on page 141.

The LAN port is connected to a single computer or the local network (internal). The WAN port is used to connect to the external network. For devices with a serial interface, the connection to the external network can also or additionally be established via the serial interface using a modem. Alternatively, the serial interface can also be used as follows: For PPP dial-in into the local network or for configuration purposes. For devices with a built-in modem (analog modem or ISDN terminal adapter), the modem can be used additionally to combine access options.

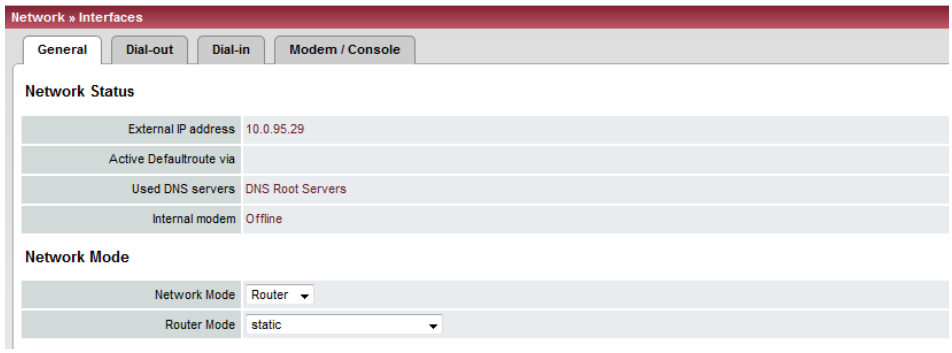
The details for this must be configured on the *General, Ethernet, Dial-out, Dial-in*, and *Modem/Console* tab pages. For a more detailed explanation of the options for using the serial interface (and a built-in modem), see “Modem/Console” on page 139.

Connecting the network interface

Connect the EAGLE mGuard to the PC via a standard Ethernet patch cable. This ensures a correct connection even when auto MDIX and auto negotiation are switched off.

The mGuard platforms have DTE interfaces (only exception: the EAGLE mGuard has a DCE network interface). Connect the mGuards to the DTE interface using an Ethernet crossover cable. Here the auto MDIX is permanently switched on, so it does not matter if the auto negotiation parameter is disabled.

6.1.1 General



Network >> Interfaces >> General		
Network Status	**External IP address**	Display only: the addresses via which the mGuard can be accessed by devices from the external network. They form the interface to other parts of the LAN or to the Internet. If the transition to the Internet takes place here, the IP addresses are usually assigned by the Internet service provider (ISP). If an IP address is assigned dynamically to the mGuard, the currently valid IP address can be found here. In *Stealth* mode, the mGuard adopts the address of the locally connected computer as its external IP.
	Active Defaultroute via	Display only: the IP address that the mGuard uses to try to reach unknown networks is displayed here. This field can contain “none” if the mGuard is in *Stealth* mode.
	Used DNS servers	Display only: the names of the DNS servers used by the mGuard for name resolution are displayed here. This information can be useful, for example, if the mGuard is using the DNS servers assigned to it by the Internet service provider.
	Internal modem	Displays the status of the internal modem (mobile network modem of the mGuard rs4000/rs2000 3G and the internal analog modem for the mGuard industrial rs)

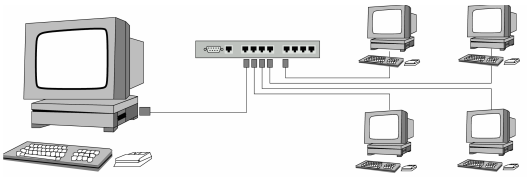
Network >> Interfaces >> General [...]		
Network Mode	**Network Mode**	**Stealth/Router** The mGuard must be set to the network mode that corresponds to its connection to the network. Depending on which network mode the mGuard is set to, the page will change together with its configuration parameters. The “Stealth” network mode is not available for the **mGuard rs2000 3G**, as it does not have a wired WAN interface. See: “Stealth (default setting mGuard rs4000/rs2000, mGuard industrial rs, mGuard smart², mGuard pci² SD, mGuard pcie² SD, mGuard pci, mGuard delta², EAGLE mGuard)” on page 108 and “Network Mode: Stealth” on page 112 “Router (default setting mGuard rs4000/rs2000 3G mGuard centerport, mGuard blade controller, mGuard delta)” on page 109 and “Network Mode: Router” on page 123
	Router Mode Only used when “Router” is selected as the network mode.	**Static/DHCP/PPPoE/PPTP/Modem[1]/Built-in Modem/Built-in mobile network modem[1]** See: “Router Mode: static” on page 110 and ““Router” network mode, “PPTP” router mode” on page 128 “Router Mode: DHCP” on page 110 and ““Router” network mode, “DHCP” router mode” on page 126 “Router Mode: PPPoE” on page 110 and ““Router” network mode, “PPPoE” router mode” on page 127 “Router Mode: PPTP” on page 110 and ““Router” network mode, “PPTP” router mode” on page 128 “Router Mode: Modem” on page 111 and ““Router" network mode, "Modem" router mode” on page 129

1 *M*odem/Built-in modem/Built-in mobile network modem is not available for all mGuard models (see “Network >> Interfaces” on page 105)

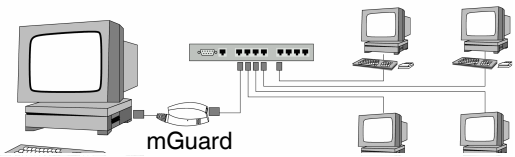
Stealth (default setting mGuard rs4000/rs2000, mGuard industrial rs, mGuard smart², mGuard pci² SD, mGuard pcie² SD, mGuard pci, mGuard delta², EAGLE mGuard)

Stealth mode (Plug-n-Protect) is used to protect a single computer or a local network with the mGuard. Important: if the mGuard is in *Stealth* network mode, it is inserted into the existing network (see figure) without changing the existing network configuration of the connected devices.

Before:



After:



(A LAN can also be on the left.)

The mGuard analyzes the active network traffic and independently configures its network connection accordingly. It then operates transparently, i.e., without the computers having to be reconfigured.

As in the other modes, firewall and VPN security functions are available.

Externally supplied DHCP data is allowed through to the connected computer.

If the mGuard is to provide services such as VPN, DNS, NTP, etc., a firewall installed on the computer must be configured to allow ICMP echo requests (ping).

In *Stealth* mode, the mGuard uses internal IP address 1.1.1.1. This can be accessed from the computer if the default gateway configured on the computer is accessible.

In *Stealth* network mode, a secondary external interface can also be configured (see “Secondary External Interface” on page 116).

For the further configuration of *Stealth* network mode, see “Network Mode: Stealth” on page 112.

Router (default setting mGuard rs4000/rs2000 3G mGuard centerport, mGuard blade controller, mGuard delta)

If the mGuard is in *Router* mode, it acts as the gateway between various subnetworks and has both an external interface (WAN port) and an internal interface (LAN port) with at least one IP address.

WAN port

The mGuard is connected to the Internet or other “external” parts of the LAN via its WAN port.

– mGuard smart^2: the WAN port is the Ethernet socket.

LAN port

The mGuard is connected to a local network or a single computer via its LAN port:

– mGuard smart^2: the LAN port is the Ethernet connector.
– mGuard pci: in *driver mode*, the LAN port is represented by the network interface of the operating system that has the network card operating system (in this example, mGuard pci).
– In *Power-over-PCI mode*, the LAN port is the LAN socket of the mGuard pcie^2 SD, mGuard pci^2 SD, mGuard pci.

As in the other modes, firewall and VPN security functions are available.

If the mGuard is operated in *Router* mode, it must be set as the default gateway on the locally connected computers.

This means that the IP address of the mGuard LAN port must be specified as the default gateway address on these computers.

NAT should be activated if the mGuard is operated in *Router* mode and establishes the connection to the Internet (see “Network >> NAT” on page 152).

Only then can the computers in the connected local network access the Internet via the mGuard. If NAT is not activated, it is possible that only VPN connections can be used.

In *Router* network mode, a secondary external interface can also be configured (see “Secondary External Interface” on page 116).

There are several Router modes, depending on the Internet connection:

– static
– DHCP
– PPPoE
– PPPT
– Modem
– Built-in Modem/Built-in mobile network modem

Router Mode: static

The IP address is fixed.

Router Mode: DHCP

The IP address is assigned via DHCP.

Router Mode: PPPoE

PPPoE mode corresponds to Router mode with DHCP but with one difference: the PPPoE protocol, which is used by many DSL modems (for DSL Internet access), is used to connect to the external network (Internet, WAN). The external IP address, which the mGuard uses for access from remote partners, is specified by the provider.

If the mGuard is operated in *PPPoE* mode, the mGuard must be set as the default gateway on the locally connected computers.

This means that the IP address of the mGuard LAN port must be specified as the default gateway address on these computers.

If the mGuard is operated in *PPPoE* mode, NAT must be activated in order to gain access to the Internet.

If NAT is not activated, it is possible that only VPN connections can be used.

For the further configuration of *PPPoE* network mode, see ""Router" network mode, "PPPoE" router mode" on page 127.

Router Mode: PPTP

Similar to *PPPoE* mode. For example, in Austria the PPTP protocol is used instead of the PPPoE protocol for DSL connections.

(PPTP is the protocol that was originally used by Microsoft for VPN connections.)

If the mGuard is operated in *PPTP* mode, the mGuard must be set as the default gateway on the locally connected computers.

This means that the IP address of the mGuard LAN port must be specified as the default gateway on these computers.

If the mGuard is operated in *PPTP* mode, NAT should be activated in order to gain access to the Internet from the local network (see "Network >> NAT" on page 152).

If NAT is not activated, it is possible that only VPN connections can be used.

For the further configuration of *PPTP* network mode, see ""Router" network mode, "PPTP" router mode" on page 128.

Router Mode: Modem

Only for *mGuard rs4000/rs2000, mGuard rs4000/rs2000 3G*, mGuard centerport, mGuard industrial rs, *mGuard blade, mGuard delta, mGuard delta²*, *EAGLE mGuard*

If *Modem* network mode is selected, the external Ethernet interface of the mGuard is deactivated and data traffic is transferred to and from the WAN via the externally accessible serial interface (serial port) of the mGuard.

An external modem, which establishes the connection to the telephone network, is connected to the serial port. The connection to the WAN or Internet is then established via the telephone network (by means of the external modem).

If the address of the mGuard is changed (e.g., by changing the network mode from *Stealth* to *Router*), the device can only be accessed via the new address. If the configuration is changed via the LAN port, confirmation of the new address is displayed before the change is applied. If configuration changes are made via the WAN port, no confirmation is displayed.

If the mode is set to *Router*, *PPPoE* or *PPTP* and you then change the IP address of the LAN port and/or the local subnet mask, make sure you specify the correct values. Otherwise, the mGuard may no longer be accessible under certain circumstances.

For the further configuration of *Built-in mobile network modem/Built-in Modem/Modem* network mode, see “"Router" network mode, "Modem" router mode” on page 129.

Router Mode: Built-in Modem

Only used for mGuard industrial rs devices **with** a built-in modem or ISDN terminal adapter

If *Built-in modem* network mode is selected, the external Ethernet interface of the mGuard is deactivated and data is transferred to and from the WAN via the built-in modem or built-in ISDN terminal adapter of the mGuard. This must be connected to the telephone network. The connection to the Internet is then established via the telephone network.

After selecting *Built-in modem*, the fields for specifying the modem connection parameters are displayed.

For the further configuration of *Built-in modem/modem* network mode, see “"Router" network mode, "Modem" router mode” on page 129.

Router Mode: Built-in mobile network modem

mGuard rs4000/rs2000 3G only.

If the *Built-in mobile network modem* is selected, data traffic is routed via the built-in mobile network modem instead of the WAN port of the mGuard.

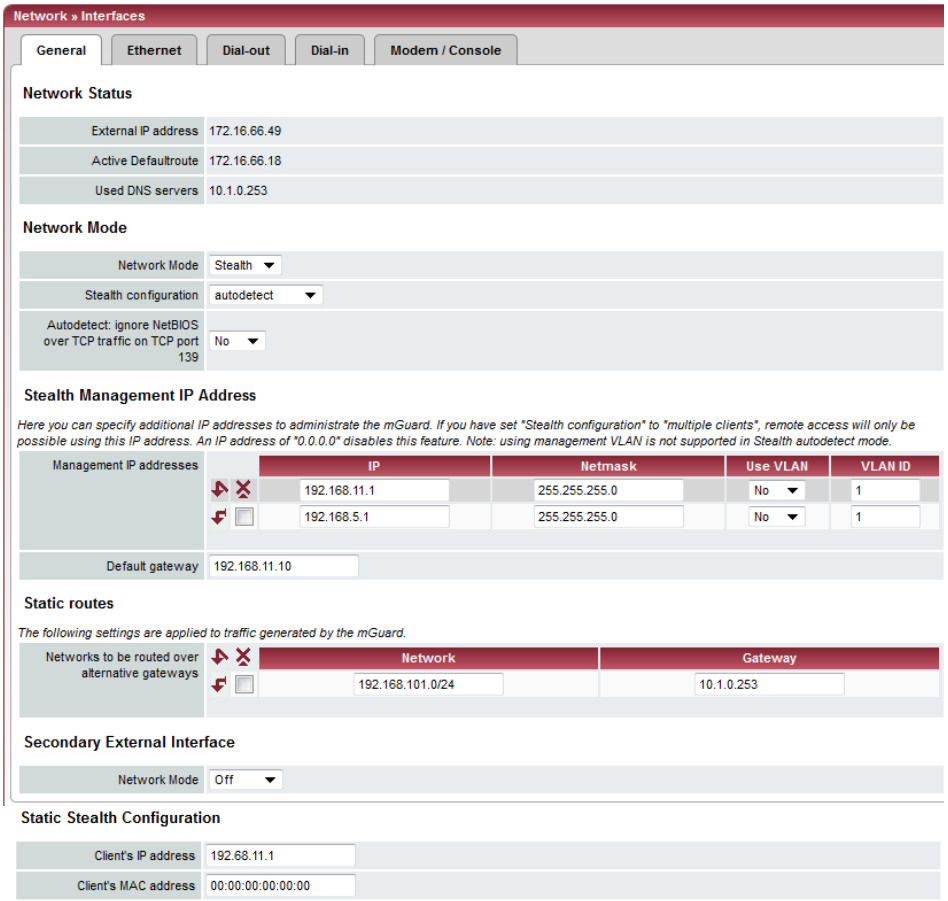
For the further configuration of *Built-in modem/modem* network mode, see “"Router" network mode, "Modem" router mode” on page 129.

Network Mode: Stealth

Default setting *mGuard rs4000/rs2000, mGuard industrial rs, mGuard smart², mGuard smart, mGuard pci² SD, mGuard pcie² SD, mGuard pci², mGuard delta², EAGLE mGuard*

When “Stealth” is selected as the network mode...

... and “static” is selected for the Stealth configura-



Network >> Interfaces >> General (“Stealth” network mode)

Network Mode

Only applies if “Stealth” is selected as the network mode.

Stealth configuration — **autodetect/static/multiple clients**

autodetect

The mGuard analyzes the network traffic and independently configures its network connection accordingly. It operates transparently.

static

If the mGuard cannot analyze the network traffic, e.g., because the locally connected computer only receives data and does not send it, then *Stealth configuration* must be set to **static**. In this case, further entry fields are available for the Static Stealth Configuration at the bottom of the page.

multiple clients

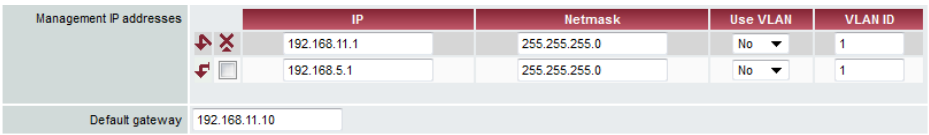
(Default) As with **autodetect**, but it is possible to connect more than one computer to the LAN port (secure port) of the mGuard, meaning that multiple IP addresses can be used at the LAN port (secure port) of the mGuard.

Autodetect: ignore NetBIOS over TCP traffic on TCP port 139 — **No/Yes**

Only with autodetect stealth configuration: if a Windows computer has more than one network card installed, it may alternate between the different IP addresses for the sender address in the data packets it sends. This applies to network packets that the computer sends to TCP port 139 (NetBIOS). As the mGuard determines the address of the computer from the sender address (and thus the address via which the mGuard can be accessed), the mGuard would have to switch back and forth, and this would hinder operation considerably. To avoid this, set this option to **Yes** if the mGuard has been connected to a computer that has these properties.

Network >> Interfaces >> General (“Stealth” network mode)[...]

Stealth Management IP Address



An additional IP address can be specified here for the administration of the mGuard.

If

– The multiple clients option is selected under *Stealth configuration*
– The client does not answer ARP requests
– No client is available

Remote access via HTTPS, SNMP, and SSH is **only** possible using this address.

With *static* Stealth configuration, the *Stealth Management IP Address* can always be accessed, even if the network card of the client PC has not been activated.

If the secondary external interface is activated (see “Secondary External Interface” on page 116), the following applies:

If the routing settings are such that data traffic to the **Stealth Management IP Address** would be routed via the secondary external interface, this would be an exclusion situation, i.e., the mGuard could no longer be administered locally.

To prevent this, the mGuard has a built-in mechanism that ensures that in such an event the Stealth Management IP Address can still be accessed by the locally connected computer (or network).

Network >> Interfaces >> General (“Stealth” network mode)[...]		
	Management IP addresses	**IP** IP address via which the mGuard can be accessed and administered. The IP address “0.0.0.0” deactivates the management IP address. Change the management IP address first before specifying any additional addresses. **Netmask** The subnet mask of the IP address above. **Use VLAN: Yes/No** IP address and subnet mask of the VLAN port. If the IP address should be within a VLAN, set this option to **Yes**. **VLAN ID** This option only applies if you set the “Stealth configuration” option to “multiple clients” . – A VLAN ID between 1 and 4095. – An explanation can be found under “VLAN” on page 364. – If you want to delete entries from the list, please note that the first entry cannot be deleted. In multi stealth mode, the external DHCP server of the mGuard cannot be used if a VLAN ID is assigned as the management IP.
	Default gateway	The default gateway of the network where the mGuard is located.
Static routes	In Stealth modes “autodetect” and “static”, the mGuard adopts the default gateway of the computer connected to its LAN port. This does not apply if a management IP address is configured with the default gateway. Alternative routes can be specified for data packets destined for the WAN that have been created by the mGuard. These include the packets from the following types of data traffic: – Download of certificate revocation lists (CRLs) – Download of a new configuration – Communication with an NTP server (for time synchronization) – Sending and receiving encrypted data packets from VPN connections – Requests to DNS servers – Syslog messages – Download of firmware updates – Download of configuration profiles from a central server (if configured) – SNMP traps	

Network >> Interfaces >> General (“Stealth” network mode)[...]

If this option is used, make the relevant entries afterwards. If it is not used, the affected data packets are routed via the default gateway specified for the client.

Network — Specify the network in CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).

Gateway — The gateway via which this network can be accessed.

The routes specified here are mandatory routes for data packets created by the mGuard. This setting has priority over other settings (see also “Network example diagram” on page 25).

Static Stealth Configuration

Client's IP address — The IP address of the computer connected to the LAN port.

Client's MAC address — The physical address of the network card of the local computer to which mGuard is connected.

- The MAC address can be determined as follows:
  In DOS (Start, Programs, Accessories, Command Prompt), enter the following command: *ipconfig /all*

The MAC address does not necessarily have to be specified. The mGuard can automatically obtain the MAC address from the client. The MAC address 0:0:0:0:0:0 must be set in order to do this. Please note that the mGuard can only forward network packets to the client once the MAC address of the client has been determined.

If no *Stealth Management IP Address* or *Client's MAC address* is configured in static Stealth mode, then DAD ARP requests are sent via the internal interface (see RFC 2131, “Dynamic Host Configuration Protocol”, Section 4.4.1)

Secondary External Interface

This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.

Only in *Router* network mode **with** *static/DHCP* router mode or *Stealth* network mode.

Only for *mGuard rs4000, mGuard centerport, mGuard industrial rs, mGuard blade, mGuard delta, EAGLE mGuard:*

In these network modes, the serial interface of the mGuard can be configured as an additional **Secondary External Interface**.

mGuard rs4000 3G only: in “Router” network mode with “Static” or “DHCP” router mode, the built-in mobile network modem of the mGuard can be configured as an additional secondary external interface.

The secondary external interface can be used to transfer data traffic *permanently* or *temporarily* to the external network (WAN).

If the secondary external interface is activated, the following applies:

Network >> Interfaces >> General (“Stealth” network mode)[...]

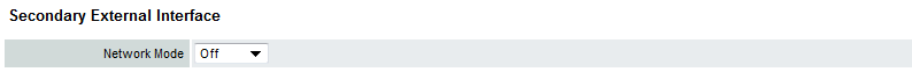
In Stealth **network mode**

Only the data traffic generated by the mGuard is subject to the routing specified for the secondary external interface, not the data traffic from a locally connected computer. Locally connected computers cannot be accessed remotely either; only the mGuard itself can be accessed remotely – if the configuration permits this.

As in Router network mode, VPN data traffic can flow to and from the locally connected computers. Because this traffic is encrypted by the mGuard, it is seen as being generated by the mGuard.

In Router **network mode**

All data traffic, i.e., from and to locally connected computers, generated by the mGuard, can be routed to the external network (WAN) via the secondary external interface.



Network Mode

Off/Modem/Built-in mobile network modem

Off

(Default). Select this setting if the operating environment of the mGuard does not require a secondary external interface. You can then use the serial interface (or the built-in modem, if present) for other purposes (see “Modem/Console” on page 139).

Modem/Built-in Modem

If you select one of these options, the secondary external interface will be used to route data traffic *permanently* or *temporarily* to the external network (WAN).

The secondary external interface is created via the serial interface of the mGuard and an external modem connected to it.

Built-in mobile network modem

Firmware 5.2 or later supports an external or internal modem as a fallback for the external interface. From Version 8.0, this also includes the internal mobile network modem of the mGuard rs4000 3G.

The modem can be used permanently as the secondary external interface.

In the event of a network error, it can also be used temporarily as a secondary external interface.

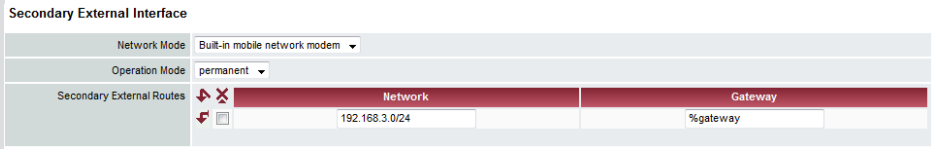
It supports dedicated routes and DNS configuration.

Network >> Interfaces >> General (“Stealth” network mode)[...]

Operation Mode

permanent/temporary

After selecting *Modem* or *Built-in Modem* network mode for the secondary external interface, the operating mode of the secondary external interface must be specified.



permanent

Data packets whose destination corresponds to the routing settings specified for the secondary external interface are always routed via this external interface. The secondary external interface is always activated.

temporary

Data packets whose destination corresponds to the routing settings specified for the secondary external interface are only routed via this external interface when additional, separately defined conditions are met. Only then is the secondary external interface activated and the routing settings for the secondary external interface take effect (see “Probes for activation” on page 120).

Secondary External Routes

Network

Specify the routing to the external network here. Multiple routes can be specified. Data packets intended for these networks are then routed to the corresponding network via the secondary external interface – in *permanent* or *temporary* mode.

Gateway

Specify the IP address (if known) of the gateway that is used for routing to the external network described above.

When you dial into the Internet using the phone number of the Internet service provider, the address of the gateway is usually not known until you have dialed in. In this case, enter **%gateway** in the field as a wildcard.

Operation Mode: permanent/temporary

In both **permanent** and **temporary** operating mode, the modem must be available to the mGuard for the secondary external interface so that the mGuard can establish a connection to the WAN (Internet) via the telephone network connected to the modem.

Which data packets are routed via the **primary external interface** (Ethernet interface) and which data packets are routed via the **secondary external interface** is determined by the routing settings that are applied for these two external interfaces. Therefore an interface can only take a data packet if the routing setting for that interface matches the destination of the data packet.

The following rules apply for routing entries:

If multiple routing entries for the destination of a data packet match, then the smallest network defined in the routing entries that matches the data packet destination determines which route this packet takes.

Example:

– The external route of the **primary** external interface is specified as 10.0.0.0/8, while the external route of the **secondary** external interface is specified as 10.1.7.0/24. Data packets to network 10.1.7.0/24 are then routed via the secondary external interface, although the routing entry for the primary external interface also matches them. Explanation: the routing entry for the secondary external interface refers to a smaller network (10.1.7.0/24 < 10.0.0.0/8).
– This rule does not apply in *Stealth* network mode with regard to the stealth management IP address (see note under “Stealth Management IP Address” on page 114).
– If the routing entries for the primary and secondary external interfaces are identical, then the secondary external interface “wins”, i.e., the data packets with a matching destination address are routed via the secondary external interface.
– The routing settings for the secondary external interface only take effect when the secondary external interface is activated. Particular attention must be paid to this if the routing entries for the primary and secondary external interfaces overlap or are identical, whereby the priority of the secondary external interface has a filter effect, with the following result: data packets whose destination matches both the primary and secondary external interfaces are always routed via the secondary external interface, but only if this is activated.
– In **temporary** mode, “activated” signifies the following: the secondary external interface is only activated when specific conditions are met, and it is only then that the routing settings of the secondary external interface take effect.
– Network address 0.0.0.0/0 generally refers to the largest definable network, i.e., the Internet.

In Router network mode, the local network connected to the mGuard can be accessed via the secondary external interface as long as the specified firewall settings allow this.

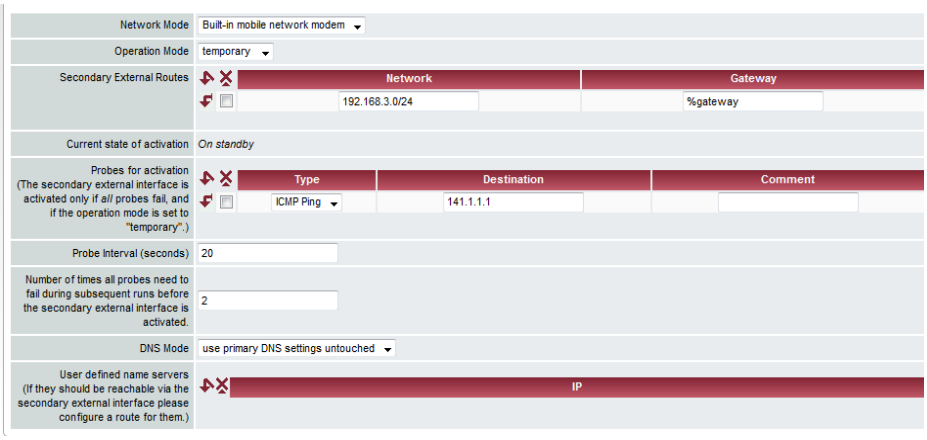
Network >> Interfaces >> General (continued); Secondary External Interface (continued)

Secondary External Interface (continued)

Network mode = “Built-in mobile network modem”

Operation Mode = temporary

Probes for activation


Network Mode
Built-in mobile network modem
Operation Mode
temporary
Secondary External Routes
Network
Gateway
192.168.3.0/24
%gateway
Current state of activation
On standby
Probes for activation (The secondary external interface is activated only if all probes fail, and if the operation mode is set to "temporary".)
Type
Destination
Comment
ICMP Ping
141.1.1.1
Probe Interval (seconds)
20
Number of times all probes need to fail during subsequent runs before the secondary external interface is activated.
2
DNS Mode
use primary DNS settings untouched
User defined name servers (If they should be reachable via the secondary external interface please configure a route for them.)
IP

If the operating mode of the secondary external interface is set to **temporary**, the following is checked using periodic ping tests: can a specific destination or destinations be reached when data packets take the route based on all the routing settings specified for the mGuard – apart from those specified for the secondary external interface? Only if **none** of the ping tests are successful does the mGuard assume that it is currently not possible to reach the destination(s) via the primary external interface (Ethernet interface or WAN port of the mGuard). In this case, the secondary external interface is activated, which results in the data packets being routed via this interface (according to the routing setting for the secondary external interface).

The secondary external interface remains activated until the mGuard detects in subsequent ping tests that the destination(s) can be reached again. If this condition is met, the data packets are routed via the **primary** external interface again and the **secondary** external interface is deactivated.

Therefore, the purpose of the ongoing ping tests is to check whether specific destinations can be reached via the primary external interface. When they cannot be reached, the secondary external interface is activated until they can be reached again.

Type/Destination

Specify the ping **Type** of the ping request packet that the mGuard is to send to the device with the IP address specified under **Destination**.

Multiple ping tests can be configured for different destinations.

Success/failure:

A ping test is successful if the mGuard receives a positive response to the sent ping request packet within 4 seconds. If the response is positive, the partner can be reached.

Network >> Interfaces >> General (continued); Secondary External Interface (continued) [...]

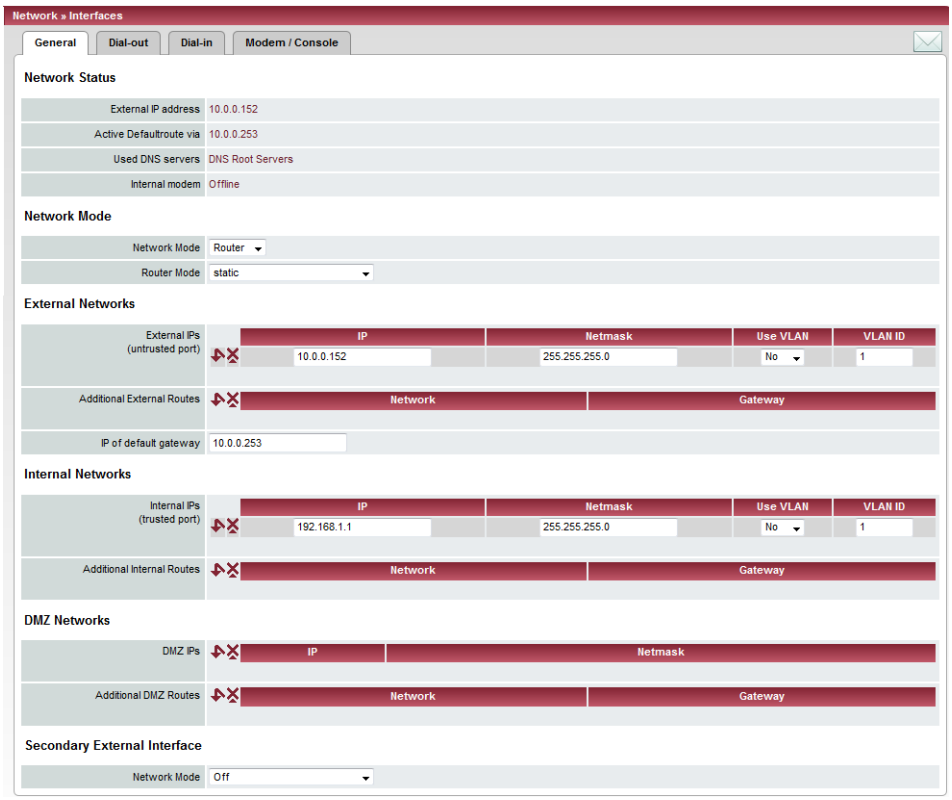
	Ping types: – IKE Ping: Determines whether a VPN gateway can be reached at the IP address specified. – ICMP Ping: Determines whether a device can be reached at the IP address specified. This is the most common ping test. However, the response to this ping test is disabled on some devices. This means that they do not respond even though they can be reached. – DNS Ping: Determines whether an operational DNS server can be reached at the IP address specified. A generic request is sent to the DNS server with the specified IP address, and every DNS server that can be reached responds to this request. Please note the following when programming ping tests: It is useful to program multiple ping tests. This is because it is possible that an individual tested service is currently undergoing maintenance. This type of scenario should not result in the secondary external interface being activated and an expensive dial-up line connection being established via the telephone network. Because the ping tests generate network traffic, the number of tests and their frequency should be kept within reasonable limits. You should also avoid activating the secondary external interface too early. The timeout time for the individual ping requests is 4 seconds. This means that after a ping test is started, the next ping test starts after 4 seconds if the previous one was unsuccessful. To take these considerations into account, make the following settings.
Probe Interval (seconds)	The ping tests defined above under **Probes for activation...** are performed one after the other. When the ping tests defined are performed once in sequence, this is known as a *test run*. Test runs are continuously repeated at intervals. The interval entered in this field specifies how long the mGuard waits after starting a test run before it starts the next test run. The test runs are not necessarily completed: as soon as one ping test in a test run is successful, the subsequent ping tests in this test run are omitted. If a test run takes longer than the interval specified, then the subsequent test run is started directly after it.

Network >> Interfaces >> General (continued); Secondary External Interface (continued) [...]	
Number of times all probes need to fail during subsequent runs before the secondary external interface is activated	Specifies how many sequentially performed test runs must return a negative result before the mGuard activates the secondary external interface. The result of a test run is negative if **none** of the ping tests it contains were successful. The number specified here also indicates how many consecutive test runs must be successful after the secondary external interface has been activated before this interface is deactivated again.
DNS Mode	Only relevant if the secondary external interface is activated in **temporary** mode: The DNS mode selected here specifies which DNS server the mGuard uses for temporary connections established via the secondary external interface. – Use primary DNS settings untouched – DNS Root Servers – Provider defined (via PPP dial-up) – User defined (from field below) **Use primary DNS settings untouched** The DNS servers defined under Network --> DNS Server (see “Network >> NAT” on page 152) are used. **DNS Root Servers** Requests are sent to the root name servers on the Internet whose IP addresses are stored on the mGuard. These addresses rarely change. **Provider defined (via PPP dial-up)** The domain name servers of the Internet service provider that provide access to the Internet are used. **User defined (from field below)** If this setting is selected, the mGuard will connect to the domain name servers listed under *User defined name servers*.
User defined name servers	The IP addresses of domain name servers can be entered in this list. The mGuard uses this list for communication via the secondary external interface – as long as the interface is activated temporarily and *User defined* is specified under **DNS Mode** (see above) in this case.

Network Mode: Router

Default setting mGuard rs4000/rs2000 3G, mGuard centerport, mGuard delta, mGuard blade controller

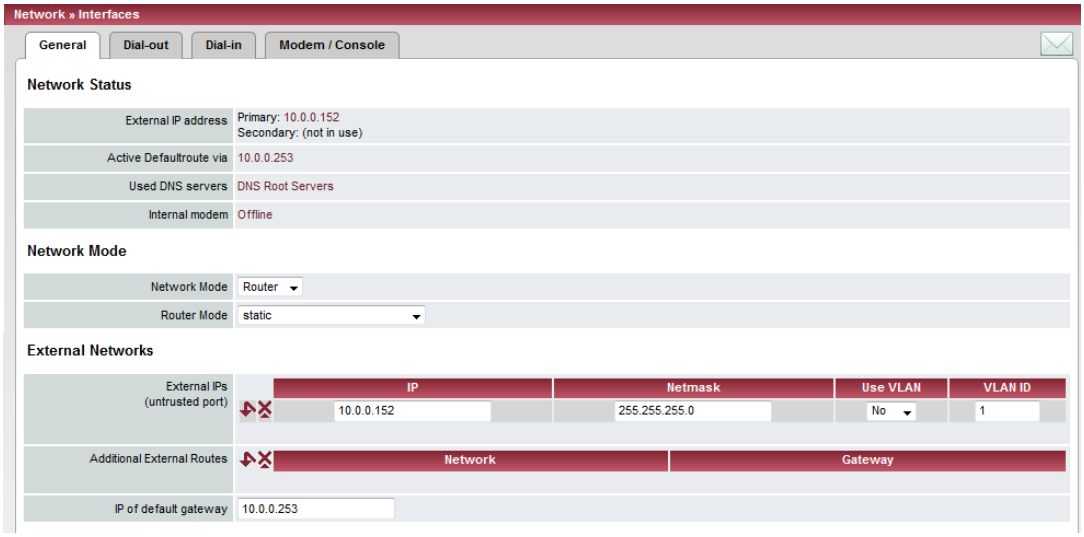
When “Router” is selected as the network mode and “static” is selected as the Router mode (see Page 125)



Network >> Interfaces >> General (“Router” network mode)		
Internal Networks	**Internal IPs (trusted port)**	The internal IP is the IP address via which the mGuard can be accessed by devices in the locally connected network. The default settings in **Router**/**PPPoE**/**PPTP**/**Modem** mode are as follows: – IP address: **192.168.1.1** – Netmask: **255.255.255.0** You can also specify other addresses via which the mGuard can be accessed by devices in the locally connected network. For example, this can be useful if the locally connected network is divided into subnetworks. Multiple devices in different subnetworks can then access the mGuard via different addresses.
	IP	IP address via which the mGuard can be accessed via its LAN port.
	Netmask	The subnet mask of the network connected to the LAN port.
	Use VLAN	If the IP address should be within a VLAN, set this option to **Yes**.

Network >> Interfaces >> General (“Router” network mode) [...]		
	VLAN ID	– A VLAN ID between 1 and 4095. – For an explanation of the term “VLAN”, please refer to the glossary on page 364. – If you want to delete entries from the list, please note that the first entry cannot be deleted.
	Additional Internal Routes	Additional routes can be defined if further subnetworks are connected to the locally connected network.
	Network	Specify the network in CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).
	Gateway	The gateway via which this network can be accessed. See also “Network example diagram” on page 25.
DMZ Networks Only available with the mGuard rs4000 3G with internal switch	**DMZ IPs**	IP address via which the mGuard can be accessed by devices in the network connected to the DMZ port. The default settings in **Router**/**PPPoE**/**PPTP**/**Modem** mode are as follows: – IP address: **192.168.3.1** – Netmask: **255.255.255.0** You can also specify other addresses via which the mGuard can be accessed by devices in the networks connected to the DMZ port. For example, this can be useful if the network connected to the DMZ port is divided into subnetworks. Multiple devices in different subnetworks can then access the mGuard via different addresses.
	IP	IP address via which the mGuard can be accessed via its DMZ port. Default: 192.168.3.1
	Netmask	The subnet mask of the network connected to the DMZ port. Default: 255.255.255.0
	Additional DMZ Routes	Additional routes can be defined if further subnetworks are connected to the DMZ.
	Network	Specify the network in CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24). Default: 192.168.3.0/24
	Gateway	The gateway via which this network can be accessed. See also “Network example diagram” on page 25. Default: 192.168.3.254
Secondary External Interface	See “Secondary External Interface” on page 116	

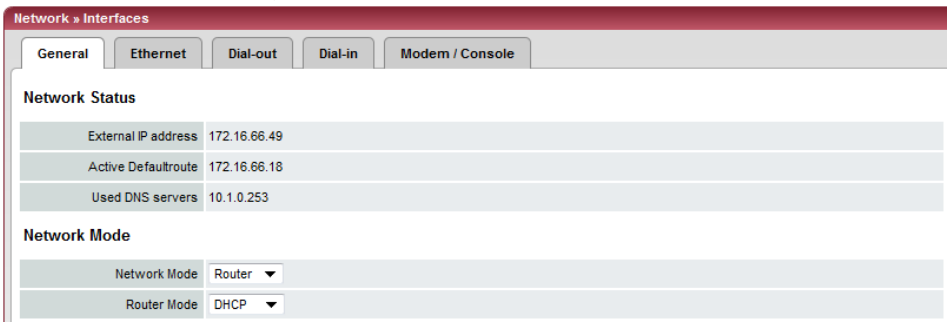
“Router” network mode, “static” router mode



Network >> Interfaces >> General (“Router” network mode, “static” router mode)		
External Networks	**External IPs (untrusted port)**	The addresses via which the mGuard can be accessed by devices on the WAN port side. If the transition to the Internet takes place here, the external IP address of the mGuard is assigned by the Internet service provider (ISP). **IP/Netmask** – IP address and subnet mask of the WAN port. **Use VLAN: Yes/No** – If the IP address should be within a VLAN, set this option to **Yes**. **VLAN ID** – A VLAN ID between 1 and 4095. – An explanation can be found under “VLAN” on page 364. – If you want to delete entries from the list, please note that the first entry cannot be deleted.
	Additional External Routes	In addition to the default route via the default gateway specified below, additional external routes can be specified. **Network/Gateway** (See “Network example diagram” on page 25)
	Internal modem	Displays the status of the internal modem (mobile network modem of the mGuard rs4000/rs2000 3G and the internal analog modem for the mGuard industrial rs)

Network >> Interfaces >> General (“Router” network mode, “static” router mode) [...]	
	IP of default gateway The IP address of a device in the local network (connected to the LAN port) or the IP address of a device in the external network (connected to the WAN port) can be specified here. If the mGuard establishes the transition to the Internet, this IP address is assigned by the Internet service provider (ISP). If the mGuard is used within the LAN, the IP address of the default gateway is assigned by the network administrator. If the local network is not known to the external router, e.g., in the event of configuration via DHCP, specify your local network under Network >> NAT (see Page 152).
DMZ Networks	**See “DMZ Networks” on page 124.**
Internal Networks	See “Internal Networks” on page 123.
Secondary External Interface	See “Secondary External Interface” on page 116.

“Router” network mode, “DHCP” router mode

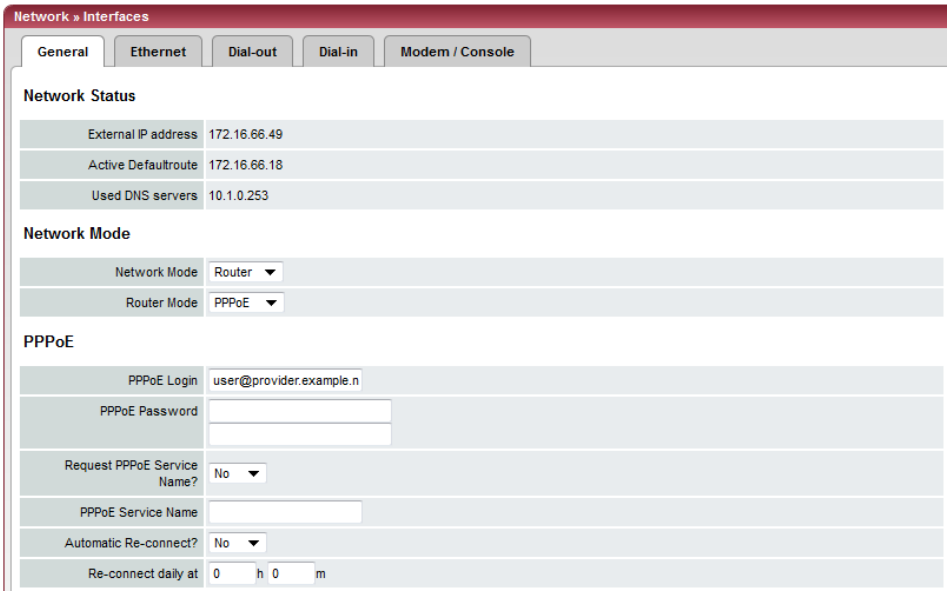


There are no additional setting options for “Router” network mode, “DHCP” router mode.

Network >> Interfaces >> General (“Router” network mode, “DHCP” router mode)	
Internal Networks	See “Internal Networks” on page 123.
Secondary External Interface	See “Secondary External Interface” on page 116

“Router” network mode, “PPPoE” router mode

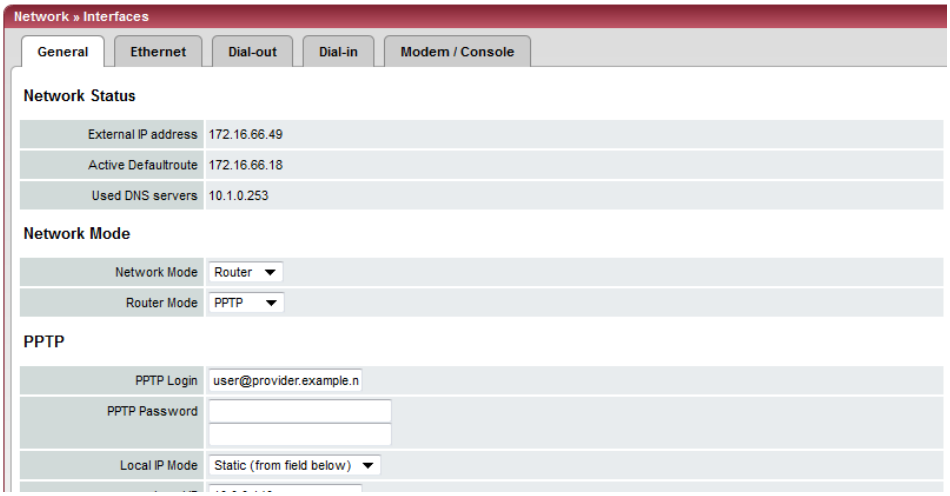
When “Router” is selected as the network mode and “PPPoE” is selected as the router mode



Network >> Interfaces >> General (“Router” network mode, “PPPoE” router mode)	
PPPoE	**For access to the Internet, the Internet service provider (ISP) provides the user with a user name (login) and password. These are requested when you attempt to establish a connection to the Internet.**
	PPPoE Login — The user name (login) that is required by the Internet service provider (ISP) when you attempt to establish a connection to the Internet.
	PPPoE Password — The password that is required by the Internet service provider when you attempt to establish a connection to the Internet.
	Request PPPoE Service Name? — When **Yes** is selected, the PPPoE client of the mGuard requests the service name specified below from the PPPoE server. Otherwise, the PPPoE service name is not used.
	PPPoE Service Name — PPPoE service name
	Automatic Re-connect? — If **Yes** is selected, specify the time in the **Re-connect daily at** field. This feature is used to schedule Internet disconnection and reconnection (as required by many Internet service providers) so that they do not interrupt normal business operations. When this function is enabled, it only takes effect if synchronization with a time server has been carried out (see “Management >> System Settings” on page 33, “Time and Date” on page 35).
	Re-connect daily at — Specified time at which the *Automatic Re-connect* function (see above) should be performed.
Internal Networks	See “Internal Networks” on page 123.
Secondary External Interface	See “Secondary External Interface” on page 116

“Router” network mode, “PPTP” router mode

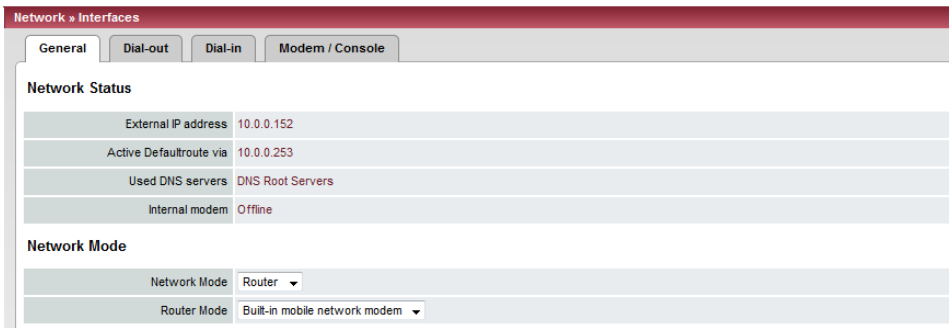
When “Router” is selected as the network mode and “PPTP” is selected as the router mode



Network >> Interfaces >> General (“Router” network mode, “PPTP” router mode)	
PPTP	**For access to the Internet, the Internet service provider (ISP) provides the user with a user name (login) and password. These are requested when you attempt to establish a connection to the Internet.**
	PPTP Login — The user name (login) that is required by the Internet service provider when you attempt to establish a connection to the Internet.
	PPTP Password — The password that is required by the Internet service provider when you attempt to establish a connection to the Internet.
	Local IP Mode — **Via DHCP:** If the address data for access to the PPTP server is provided by the Internet service provider via DHCP, select **Via DHCP**. In this case, no entry is required under **Local IP**. **Static (from field below):** If the address data for access to the PPTP server is **not** supplied by the Internet service provider via DHCP, the local IP address must be specified.
	Local IP — The IP address via which the mGuard can be accessed by the PPTP server.
	Modem IP — The address of the PPTP server of the Internet service provider.
Internal Networks	See “Internal Networks” on page 123.
Secondary External Interface	See “Secondary External Interface” on page 116
This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.	

"Router" network mode, "Modem" router mode

Only *mGuard rs4000 3G, mGuard rs4000*, *mGuard centerport*, mGuard industrial rs, *mGuard blade, mGuard delta*[2], *mGuard delta, EAGLE mGuard*



Network >> Interfaces >> General ("Router" network mode, "Modem" router mode)

Modem/Built-in Modem/Built-in mobile network modem

Modem network mode is available for: *mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs, mGuard blade, EAGLE mGuard, mGuard delta*

The **Built-in Modem** network mode is also available for the: *mGuard industrial rs*, if it has a built-in modem or a built-in ISDN terminal adapter (optional).

The **Built-in mobile network modem** is also available for the *mGuard rs4000 3G* and *mGuard rs2000 3G*.

For all of the devices mentioned above, data traffic is routed via the serial interface and not via the mGuard WAN port when in *Modem* or *Built-in (mobile network) Modem* network mode and from there it continues as follows.

– A - data traffic is routed via the externally accessible serial interface (serial port), to which an external modem must be connected.
– B – data traffic is routed via the built-in (mobile network) modem/built-in ISDN terminal adapter, if available.

In both cases, the connection to the Internet service provider and therefore the Internet is established via the telephone network using a modem or ISDN terminal adapter.

In *Modem* network mode, the serial interface of the mGuard is not available for the PPP dial-in option or for configuration purposes (see “Modem/Console” on page 139).

After selecting **Modem**[1] as the network mode, specify the required parameters for the modem connection on the **Dial-out** and/or **Dial-in** tab pages (see “Dial-out” on page 130 and “Dial-in” on page 136).

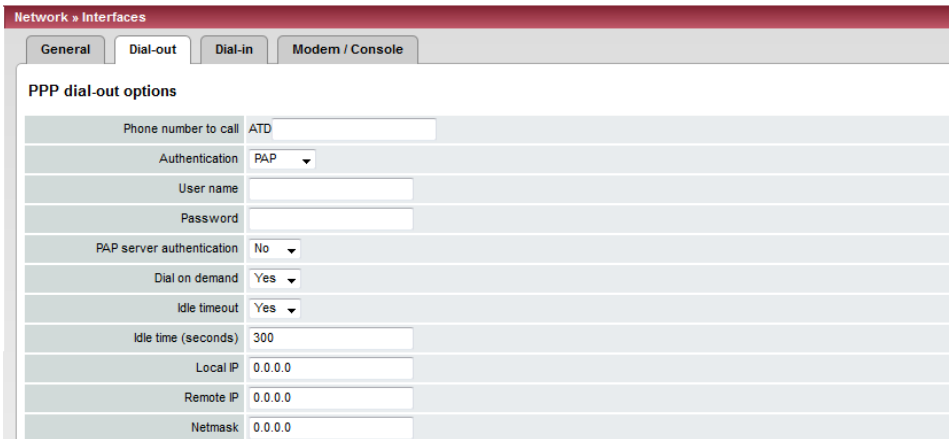
Enter the connection settings for an external modem on the *Modem/Console* tab page (see “Modem/Console” on page 139).

The configuration of the internal networks is described in the next section.

1 In the case of the mGuard industrial rs with built-in modem or ISDN terminal adapter, **Built-in Modem** is available as an option and in the case of mGuard rs4000 3G **Built-in mobile network modem** is available as an option

6.1.2 Dial-out

Only *mGuard rs4000 3G, mGuard rs4000*, *mGuard centerport*, *mGuard industrial rs, mGuard blade, mGuard delta², mGuard delta, EAGLE mGuard*



Network >> Interfaces >> Dial-out

PPP dial-out options

This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.

These settings are only necessary when the mGuard is to establish a data link to the WAN (Internet) via one of these interfaces.

– Via the primary external interface (*Modem* or *Built-in (mobile network) Modem* network mode)
– Via the secondary external interface (also available in *Stealth* or *Router* network mode)

Phone number to call

Phone number of the Internet service provider. The connection to the Internet is established after establishing the telephone connection.

Command syntax: together with the previously set ATD modem command for dialing, the following dial sequence, for example, is created for the connected modem: ATD765432.

A compatible pulse dialing procedure that works in all scenarios is used as standard.

Special dial characters can be used in the dial sequence.

Network >> Interfaces >> Dial-out[...]

HAYES special dial characters

– **W:** instructs the modem to insert a dialing pause at this point until the dial tone can be heard.

  Used when the modem is connected to a private branch exchange. An external line must be obtained first for outgoing calls by dialing a specific number (e.g., 0) before the phone number of the relevant subscriber can be dialed.

  Example: ATD0W765432

– **T**: switch to tone dialing.

  Insert the special dial character T before the phone number if the faster tone dialing procedure is to be used (with tone-compatible telephone connections). Example: ATDT765432

Authentication

PAP/CHAP/None

PAP = Password Authentication Protocol, CHAP = Challenge Handshake Authentication Protocol. These terms describe procedures for the secure transmission of authentication data using the Point-to-Point Protocol.

If the Internet service provider requires the user to login using a user name and password, then PAP or CHAP is used as the authentication method. The user name, password, and any other data that must be specified by the user to establish a connection to the Internet are given to the user by the Internet service provider.

The corresponding fields are displayed depending on whether **PAP**, **CHAP** or **None** is selected. Enter the corresponding data in these fields.

If authentication is via PAP:

User name

User name specified during Internet service provider login to access the Internet.

Password

Password specified during Internet service provider login to access the Internet.

Network >> Interfaces >> Dial-out[...]

PAP server authentication	**Yes/No** The following two entry fields are shown when **Yes** is selected:
Server user name **Server password**	User name and password that the mGuard requests from the server. The mGuard only allows the connection if the server returns the agreed user name/password combination.
Subsequent fields	See under "If "None" is selected as the authentication method" on page 133.

If authentication is via CHAP:

Local name	A name for the mGuard that it uses to log into the Internet service provider. The service provider may have several customers and it uses this name to identify who is attempting to dial in. After the mGuard has logged into the Internet service provider with this name, the service provider also compares the password specified for client authentication (see below). The connection can only be established successfully if the name is known to the service provider and the password matches.
Remote name	A name given to the mGuard by the Internet service provider for identification purposes. The mGuard will not establish a connection to the service provider if the ISP does not give the correct name.
Secret for client authentication	Password that must be specified during Internet service provider login to access the Internet.
CHAP server authentication	**Yes/No** The following two entry fields are shown when **Yes** is selected:
Secret for server authentication	Password that the mGuard requests from the server. The mGuard only allows the connection if the server returns the agreed password.

Network >> Interfaces >> Dial-out[...]

Subsequent fields

See under "If "None" is selected as the authentication method" on page 133.

If "None" is selected as the authentication method

In this case, the fields that relate to the PAP or CHAP authentication methods are hidden.

Only the fields that define further settings remain visible below.

Other common settings

Network >> Interfaces >> Dial-out

PPP dial-out options

Dial on demand

Yes/No

Whether *Yes* or *No*: the telephone connection is always established by the mGuard.

If set to **Yes** (default): this setting is useful for telephone connections where costs are calculated according to the connection time.

The mGuard only commands the modem to establish a telephone connection when network packets are actually to be transferred. It also instructs the modem to terminate the telephone connection as soon as no more network packets are to be transmitted for a specific time (see value in *Idle timeout* field). By doing this, however, the mGuard is not constantly available externally, i.e., for incoming data packets.

Network >> Interfaces >> Dial-out[...]

The mGuard also often or sporadically establishes a connection via the modem, or keeps a connection longer, if the following conditions apply:

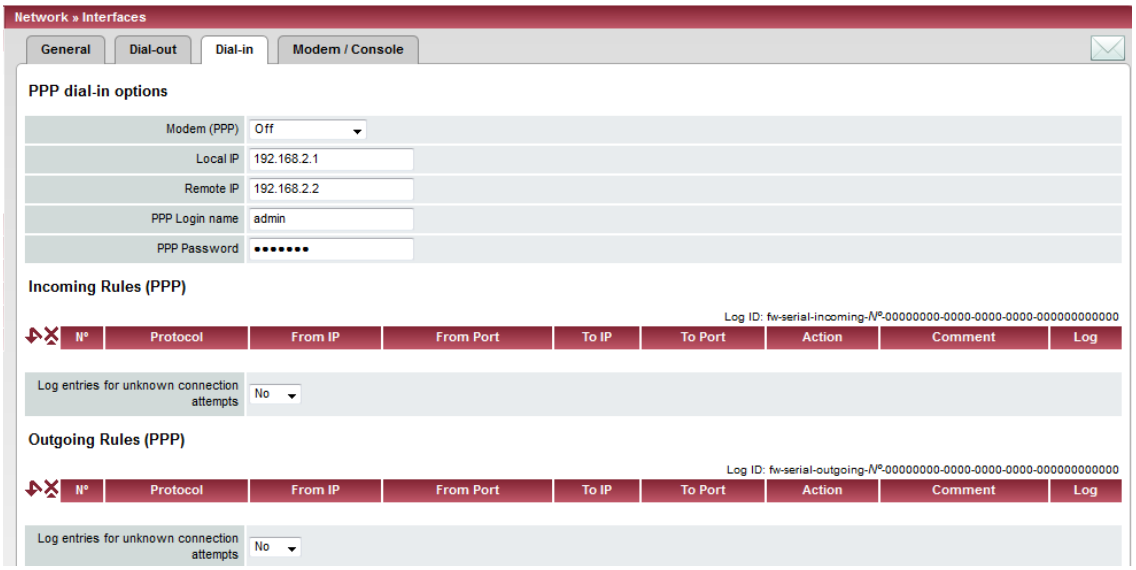
- Often: the mGuard is configured so that it synchronizes its system time (date and time) regularly with an external NTP server.
- Sporadically: the mGuard acts as a DNS server and must perform a DNS request for a client.
- After a restart: an active VPN connection is set to **Started**. If this is the case, the mGuard establishes a connection after every restart.
- After a restart: for an active VPN connection, the gateway of the partner is specified as the host name. After a restart, the mGuard must request the IP address that corresponds to the host name from a DNS server.
- Often: VPN connections are set up and DPD messages are sent regularly (see “Dead Peer Detection” on page 282).
- Often: the mGuard is configured to send its external IP address regularly to a DNS service, e.g., DynDNS, so that it can still be accessed via its host name.
- Often: the IP addresses of partner VPN gateways must be requested from the DynDNS service or they must be kept up-to-date by new queries.
- Sporadically: the mGuard is configured so that SNMP traps are sent to the remote server.
- Sporadically: the mGuard is configured to permit and accept remote access via HTTPS, SSH or SNMP. (The mGuard then sends reply packets to every IP address from which an access attempt is made (if the firewall rules permit this access)).
- Often: the mGuard is configured to connect to an HTTPS server at regular intervals in order to download any configuration profiles available there (see “Management >> Central Management” on page 91).

When **No** is selected, the mGuard establishes a telephone connection using the connected modem as soon as possible after a restart or activation of *Modem* network mode. This remains permanently in place, regardless of whether or not data is transmitted. If the telephone connection is then interrupted, the mGuard attempts to restore it immediately. Thus a permanent connection is created, like a permanent line. By doing this, the mGuard is constantly available externally, i.e., for incoming data packets.

Network >> Interfaces >> Dial-out[...]		
	Idle timeout	**Yes/No** Only considered when *Dial on demand* is set to **Yes**. When set to **Yes** (default), the mGuard terminates the telephone connection as soon as no data traffic is transmitted over the time period specified under *Idle time*. The mGuard gives the connected modem the relevant command for terminating the telephone connection. When set to **No**, the mGuard does not give the connected modem a command for terminating the telephone connection.
	Idle time (seconds)	Default: 300. If there is still no data traffic after the time specified here has elapsed, the mGuard can terminate the telephone connection (see above under *Idle timeout*).
	Local IP	IP address of the serial interface of the mGuard that now acts as the WAN interface. If this IP address is assigned dynamically by the Internet service provider, use the preset value: 0.0.0.0. Otherwise, e.g., for the assignment of a fixed IP address, enter this here.
	Remote IP	IP address of the partner. When connecting to the Internet, this is the IP address of the Internet service provider, which is used to provide access to the Internet. As the Point-to-Point Protocol (PPP) is used for the connection, the IP address does not usually have to be specified. This means you can use the preset value: 0.0.0.0.
	Netmask	The subnet mask specified here belongs to both the *Local IP* address and the *Remote IP* address. Normally all three values (*Local IP, Remote IP, Netmask*) are either fixed or remain set to 0.0.0.0. Enter the connection settings for an external modem on the *Modem/Console* tab page (see “Modem/Console” on page 139).

6.1.3 Dial-in

Only *mGuard rs4000 3G, mGuard rs4000, mGuard centerport*, mGuard industrial rs, *mGuard blade, mGuard delta², mGuard delta, EAGLE mGuard*



Network >> Interfaces >> Dial-in

PPP dial-in options

This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.

Only *mGuard rs4000 3G, mGuard rs4000, mGuard centerport*, mGuard industrial rs, *mGuard blade, mGuard delta², mGuard delta, EAGLE mGuard*

Should only be configured if the mGuard is to permit PPP dial-in via one of the following:

– A modem connected to the serial interface
– A built-in modem (as option for the mGuard industrial rs)
– A built-in mobile network modem (for *mGuard rs4000 3G, mGuard rs4000*).

PPP dial-in can be used to access the LAN (or the mGuard for configuration purposes) (see “Modem/Console” on page 139).

If the modem is used for dialing out by acting as the primary external interface (*Modem* network mode) of the mGuard or as its secondary external interface (when activated in *Stealth* or *Router* network mode), it is not available for the PPP dial-in option.

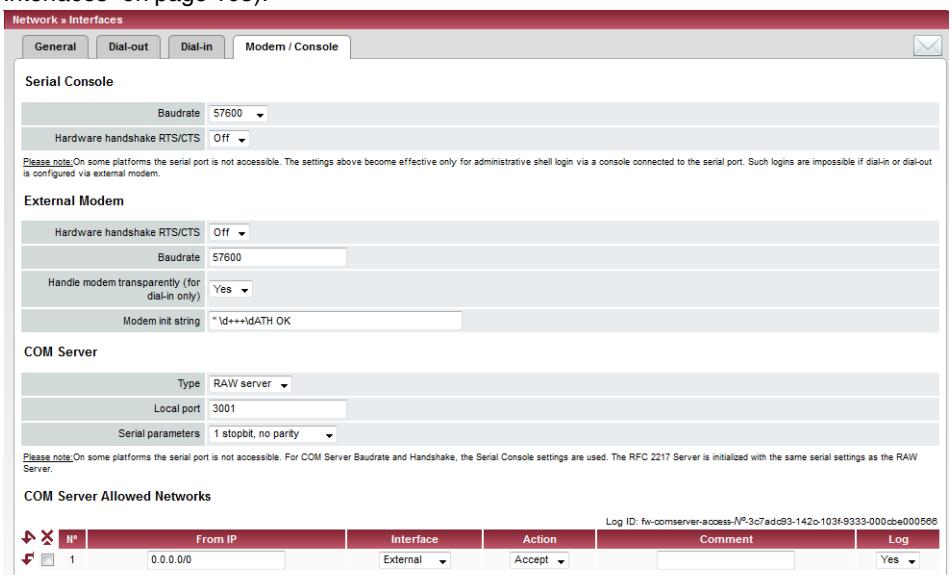
Network >> Interfaces >> Dial-in [...]	
Modem (PPP)	**Only** *mGuard rs4000 3G, mGuard rs4000, mGuard industrial rs* **(without built-in modem/ISDN TA),** *mGuard delta[2], mGuard delta, EAGLE mGuard* **Off/On** This option **must** be set to “Off” if no serial interface is to be used for the PPP dial-in option. If this option is set to **On**, the PPP dial-in option is available. The connection settings for the connected external modem should be made on the *Modem/Console* tab page.
Modem (PPP)	**Only for** *mGuard industrial rs* **(with built-in modem/ISDN TA)** **Off/Built-in Modem/External Modem** This option **must** be set to **Off** if no serial interface should be used for the PPP dial-in option. If this option is set to **External Modem**, the PPP dial-in option is available. An external modem must then be connected to the serial interface. The connection settings for the connected external modem should be made on the *Modem/Console* tab page. If this option is set to **Built-in Modem**, the PPP dial-in option is available. In this case, the modem connection is not established via the *serial* socket on the front. Instead it is established via the terminal strip on the bottom where the built-in modem or ISDN terminal adapter is connected to the telephone network. The connection settings for the built-in modem should be made on the *Modem/Console* tab page. If the **Built-in Modem** option is used, the serial interface can also be used. For the options for using the serial interface, see “Modem/Console” on page 139.
Local IP	IP address of the mGuard via which it can be accessed for a PPP connection.
Remote IP	IP address of the partner of the PPP connection.
PPP Login name	Login name that must be specified by the PPP partner in order to access the mGuard via a PPP connection.
PPP Password	The password that must be specified by the PPP partner in order to access the mGuard via a PPP connection.

Network >> Interfaces >> Dial-in [...]		
Incoming Rules (PPP)	Firewall rules for PPP connections to the LAN interface. If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored. The following options are available:	
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols
	From/To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).
	From/To Port	(Only evaluated for TCP and UDP protocols.) **any** refers to any port. **startport:endport** (e.g., 110:120) refers to a port area. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default settings).
	Log entries for unknown connection attempts	Yes/No When set to **Yes**, all connection attempts that are not covered by the rules defined above are logged.
Outgoing Rules (PPP)	Firewall rules for outgoing PPP connections from the LAN interface. The parameters correspond to those under *Incoming Rules (PPP)*. These outgoing rules apply to data packets that are sent out via a data link initiated by PPP dial-in.	

6.1.4 Modem/Console

Only *mGuard rs4000 3G, mGuard rs2000 3G (only console), mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs, mGuard smart*^{2}, *mGuard delta*^{2} (**not** *mGuard smart, mGuard pci*^{2} *SD, mGuard blade, mGuard delta, EAGLE mGuard)*

Some mGuard models have a serial interface that can be accessed externally, while the mGuard industrial rs is also available with a built-in modem as an option (see “Network >> Interfaces” on page 105).



Options for using the serial interface

The serial interface can be used alternatively as follows:

Primary external interface (This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000)

As a **primary external interface**, if the network mode is set to *Modem* under *Network* >> *Interfaces* on the *General* tab page (see “Network >> Interfaces” on page 105 and “” on page 106).

In this case, data traffic is not processed via the WAN port (Ethernet interface), but via the serial interface.

Secondary external interface (This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000)

As a **secondary external interface**, if *Secondary External Interface* is activated and *Modem* is selected under *Network* >> *Interfaces* on the *General* tab page (see “Network >> Interfaces” on page 105 and “” on page 106).

In this case, data traffic is processed (permanently or temporarily) via the serial interface.

For dialing in to the LAN or for configuration purposes (This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000)

Used for **dialing in to the LAN or for configuration purposes** (see also “Dial-in” on page 136). The following options are available:

– A modem is connected to the serial interface of the mGuard. This modem is connected to the telephone network (fixed-line or GSM network).

  (The connection to the telephone network is established via the terminal strip on the bottom of the device for the mGuard industrial rs **with** built-in modem or ISDN terminal adapter.)

  This enables a remote PC that is also connected to the telephone network via a modem or ISDN adapter to establish a PPP (Point-to Point Protocol) dial-up line connection to the mGuard.

This method is referred to as a PPP dial-in option. It can be used for access to the LAN, which is located behind the mGuard or for configuration of the mGuard. *Dial-in* is the interface definition used for this connection type in firewall selection lists.

In order to access the LAN with a Windows computer using the dial-up line connection, a network connection must be set up on this computer in which the dial-up line connection to the mGuard is defined. In addition, the IP address of the mGuard (or its host name) must be defined as the gateway for this connection so that the connections to the LAN can be routed via this address.

To access the web configuration interface of the mGuard, you must enter the IP address of the mGuard (or its host name) in the address line of the web browser.

– The serial interface of the mGuard is connected to the serial interface of a PC.

  On the PC, the connection to the mGuard is established using a terminal program and the configuration is implemented using the command line of the mGuard.

If an external modem is connected to the serial interface, you may have to enter corresponding settings below under *External Modem*, regardless of the use of the serial port and the modem connected to it.

Network >> Interfaces >> Modem/Console

Serial Console

The following settings for the *Baudrate* and *Hardware handshake* are only valid for a configuration connection where a terminal or PC with terminal program is connected to the serial interface as described above.

The settings are not valid when an external modem is connected. Settings for this are made further down under *External Modem*.

Baudrate	The transmission speed of the serial interface is specified via the selection list.
Hardware handshake RTS/CTS	**Off/On** When set to **On**, flow is controlled by means of RTS and CTS signals.

Network >> Interfaces >> Modem/Console [...]		
	Serial console via USB	No/Yes
	(Only for mGuard smart²)	When **No** is selected, the mGuard smart² uses the USB connection solely as a power supply. When **Yes** is selected, the mGuard smart² provides an additional serial interface for the connected computer through the USB interface. The serial interface can be accessed on the computer using a terminal program. The mGuard smart² provides a console through the serial interface, which can then be used in the terminal program. Windows requires a special driver. This can be directly downloaded from the mGuard. The relevant link is located on the right-hand side next to the “Serial console via USB” drop-down menu.
External Modem This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.	**Hardware handshake RTS/CTS**	**Off/On** When set to **On**, flow is controlled by means of RTS and CTS signals for PPP connections.
	Baudrate	Default: 57600. Transmission speed for communication between the mGuard and modem via the serial connecting cable between both devices. This value should be set to the highest value supported by the modem. If the value is set lower than the maximum possible speed that the modem can reach on the telephone line, the telephone line will not be used to its full potential.
	Handle modem transparently (for dial-in only)	**Yes/No** If the external modem is used for dial-in (see Page 136), **Yes** means that the mGuard does not initialize the modem. The subsequently configured modem initialization sequence is not observed. Thus, either a modem is connected which can answer calls itself (default profile of the modem contains “auto answer”) or a null modem cable to a computer can be used instead of the modem, and PPP protocol is used over this.
	Modem init string	Specifies the initialization sequence that the mGuard sends to the connected modem. Default: *''\d+++\dATH OK* Consult the modem user manual for the initialization sequence for this modem.
	The initialization sequence is a sequence of character strings expected by the modem and commands that are then sent to the modem so that the modem can establish a connection.	

The preset initialization sequence has the following meaning:

'' (two simple quotation marks placed directly after one another)	The empty character string inside the quotation marks means that the mGuard does not initially expect any information from the connected modem, but instead sends the following text directly to the modem.
\d+++\dATH	The mGuard sends this character string to the modem in order to determine whether the modem is ready to accept commands.
OK	Specifies that the mGuard expects the *OK* character string from the modem as a response to *\d+++\dATH*.

On many modem models it is possible to save modem default settings to the modem itself. However, this option should not be used.

Initialization sequences should be configured externally instead (i.e., on the mGuard). In the event of a modem fault, the modem can then be replaced quickly and smoothly without changing the modem default settings.

If the external modem is to be used for incoming calls without the modem default settings being entered accordingly, then you have to inform the modem that it should accept incoming calls after it rings.

If using the extended HAYES command set, append the character string " *AT&S0=1 OK*" (a space followed by "*AT&S0=1*", followed by a space, followed by "*OK*") to the initialization sequence.

Some external modems, depending on their default settings, require a physical connection to the DTR cable of the serial interface in order to operate correctly.

Because the mGuard models do not provide this cable at the external serial interface, the character string *" AT&D0 OK"* (a space followed by *"AT&D0"*, followed by a space, followed by *"OK"*) must be appended to the above initialization sequence. According to the extended HAYES command set, this sequence means that the modem does not use the DTR cable.

If the external modem is to be used for outgoing calls, it is connected to a private branch exchange, and if this private branch exchange does not generate a dial tone after the connection is opened, then the modem must be instructed not to wait for a dial tone before dialing.

In this case, append the character string " *ATX3 OK*" (a space followed by "*ATX3"*, followed by a space, followed by "*OK*") to the initialization sequence.

In order to wait for the dial tone, the control character "*W*" should be inserted in the *Phone number to call* after the digit for dialing an outside line.

COM server for mGuard platforms with serial interface

The mGuard platforms with a serial interface have an integrated COM server as of firmware 8.0 and later. This enables serial interface data exchange via an IP connection.

Three options are available.

– **RFC 2217** (Telnet server, complies with RFC 2217).

  In this mode, the serial interface can be configured via client software in the network. The Telnet server is available via the port which is defined under “Local Port” .

– **RAW client**

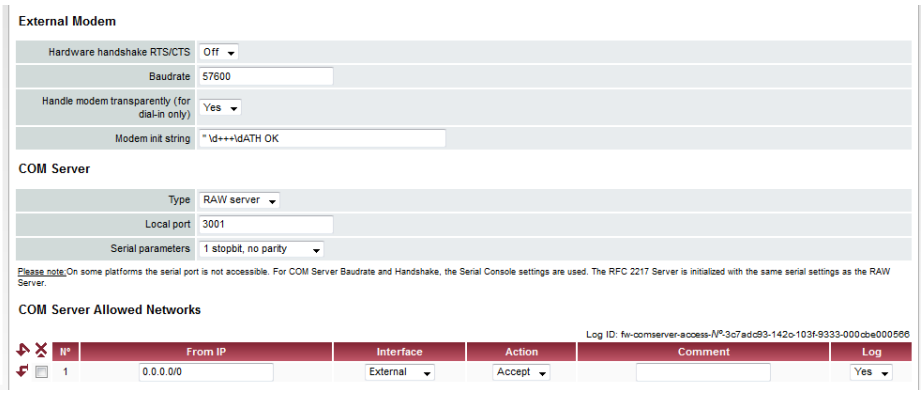
  In this mode, the mGuard initiates a connection to the address which is set under “Remote IP address” . The connection is established via the port which is configured under “Remote Port” .

  The interface can be configured here (“Serial parameters”). The settings of the serial console are used for the baud rate and the hardware handshake (see “External Modem” under “Network >> Interfaces >> Modem/Console”).

– **RAW server**

  Behaves in the same way as the RAW client. However, the RAW server responds to incoming connections via the port which is configured under “Local Port” .

Additional settings for mGuard platforms with serial interface



Network >> Interfaces >> Modem/Console (mGuard platforms with serial interface)		
COM server	**Type**	Here you can select the way that the COM server should operate. Possible options are: RFC 2217, RAW client, RAW server.
	Local Port	Defines the port that the COM server should respond to. Is available when the type is set to RFC 2217 or RAW server. Values: 1 – 65535. Default: 3001
	Remote IP address	Defines the remote IP address of a RAW client. Is available when the type is set to RAW client. Default: 10.1.0.254.

Network >> Interfaces >> Modem/Console (mGuard platforms with serial interface) [...]		
	Remote Port	Defines the port to which the RAW client sends the data. Is available when the type is set to RAW client. Values: 1 – 65535. Default: 3001.
	Serial parameters	Defines the parity and stop bits for the serial interface. The general packet length of the serial interface is 8 bits. – 1 stop bit, no parity (default) – 1 stop bit, even parity – 1 stop bit, odd parity – 2 stop bits, no parity – 2 stop bits, even parity – 2 stop bits, odd parity
COM Server Allowed Networks	Access rules can be defined for the COM server to prevent unauthorized access to it. The default rule does not allow any access via the external interface.	
	From IP	0.0.0.0/0 means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).
	Interfaces	Interface for which the rule should apply. Values: None, External, DMZ, VPN
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back. The sender is informed of their rejection. **Drop** means that the data packets are not permitted to pass through. The sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each firewall rule you can specify whether the event is to be logged if the rule is applied.

For the mGuard industrial rs with built-in modem/built-in ISDN modem (ISDN terminal adapter)

The mGuard industrial rs is available with a built-in analog modem/built-in ISDN terminal adapter as an option. The built-in modem or built-in ISDN terminal adapter can be used as follows:

Primary External Interface

– As a **primary external interface**, if the network mode is set to *Built-in Modem* under *Network >> Interfaces* on the *General* tab page (see “Network >> Interfaces” on page 105 and “” on page 106). In this case, data traffic is not processed via the WAN port (Ethernet interface), but via this modem.

Secondary External Interface

– As a **secondary external interface**, if *Secondary External Interface* is activated and *Built-in Modem* is selected under *Network >> Interfaces* on the *General* tab page (see “Network >> Interfaces” on page 105 and “” on page 106). In this case data traffic is also processed via the serial interface.

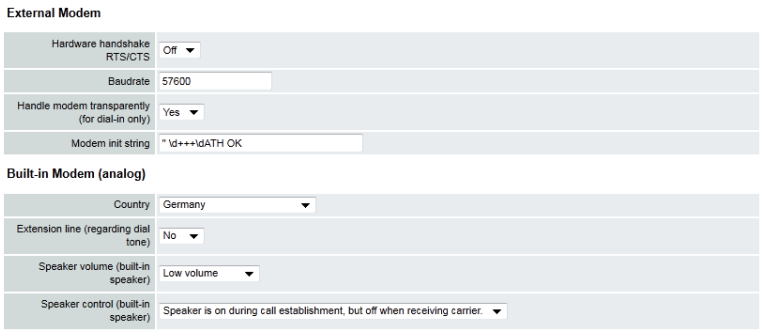
PPP dial-in options

– For the PPP dial-in option (see “Options for using the serial interface” on page 139).

Please note that the serial interface of the device also provides similar options for use (see above). Therefore on an mGuard industrial rs with a built-in modem, normal data traffic can be routed via a modem connection (*Modem* network mode) and a second modem connection can be used simultaneously for the PPP dial-in option, for example.

For the mGuard industrial rs with built-in modem

Additionally for the mGuard industrial rs with built-in modem (analog)



Network >> Interfaces >> Modem/Console (for the mGuard industrial rs with built-in modem)		
External Modem	**As for the mGuard rs4000 3G, mGuard industrial rs (without built-in modem), mGuard delta^2, mGuard centerport, mGuard blade, mGuard delta, EAGLE mGuard:** Configuration as above for **External Modem** (see “External Modem” on page 141).	
Built-in Modem (analog)	**Country**	The country where the mGuard with built-in modem is operated must be specified here. This ensures that the built-in modem operates according to the applicable remote access guidelines in the respective country and that it recognizes and uses dial tones correctly, for example.
	Extension line (regarding dial tone)	Yes/No When set to **No**, the mGuard waits for the dial tone when the telephone network is accessed and the mGuard is calling the partner. When set to **Yes**, the mGuard does not wait for a dial tone. Instead it begins dialing the partner immediately. This procedure may be necessary if the built-in modem of the mGuard is connected to a private branch exchange that does not emit a dial tone when it is “picked up”. When a specific number must be dialed to access an external line, e.g., “0”, this number should be added to the start of the desired partner phone number that is to be dialed.
	Speaker volume (built-in speaker)	
	Speaker control (built-in speaker)	These two settings specify which sounds should be emitted by the mGuard speaker and at what volume.

For the mGuard industrial rs with built-in ISDN terminal adapter

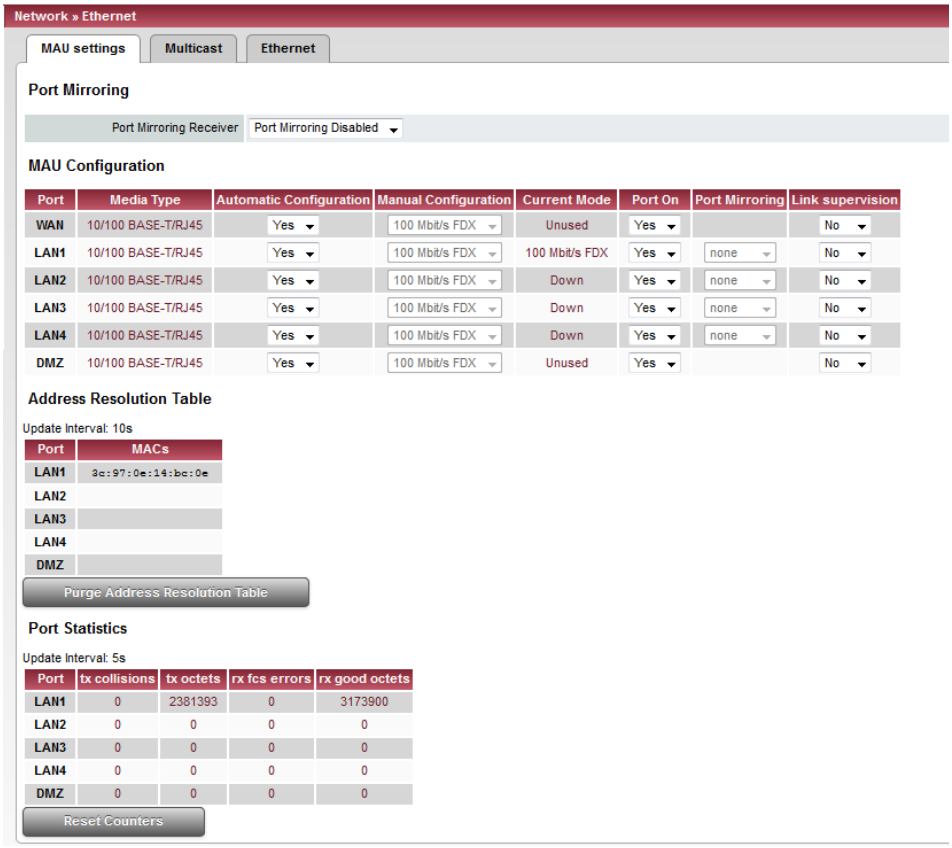
Additionally for the mGuard industrial rs with built-in modem (ISDN)

Network >> Interfaces >> Modem/Console (for the mGuard industrial rs with ISDN terminal adapter)		
External Modem	**As for the mGuard rs4000, mGuard industrial rs (without built-in modem), mGuard centerport, mGuard blade, mGuard delta, EAGLE mGuard:** Configuration as above for **External Modem** (see “External Modem” on page 141).	
Built-in Modem (ISDN)	**1st MSN**	For outgoing calls, the mGuard transmits the MSN (Multiple Subscriber Number) entered here to the called partner. In addition, the mGuard can receive incoming calls via this MSN (provided dial-in operation is enabled – see *General* tab page). Maximum of 25 alphanumeric characters; the following special characters can be used: *****, **#**, **:** (colon)
	2nd MSN	If the mGuard should also receive incoming calls via another number for dial-in operation (if enabled), enter the second MSN here.
	ISDN protocol	The EuroISDN protocol (also known as NET3) is used in Germany and many other European countries. Otherwise the ISDN protocol should be specified according to the country. If necessary, this must be requested from the relevant phone company.
	Layer-2 protocol	The set of rules used by the ISDN terminal adapter of the local mGuard to communicate with its ISDN partner. This generally is the ISDN modem of the Internet service provider used to establish the connection to the Internet. It must be requested from the Internet service provider. PPP/ML-PPP is often used.

6.2 Network >> Ethernet

Only available with the mGuard rs4000 3G.

6.2.1 MAU settings



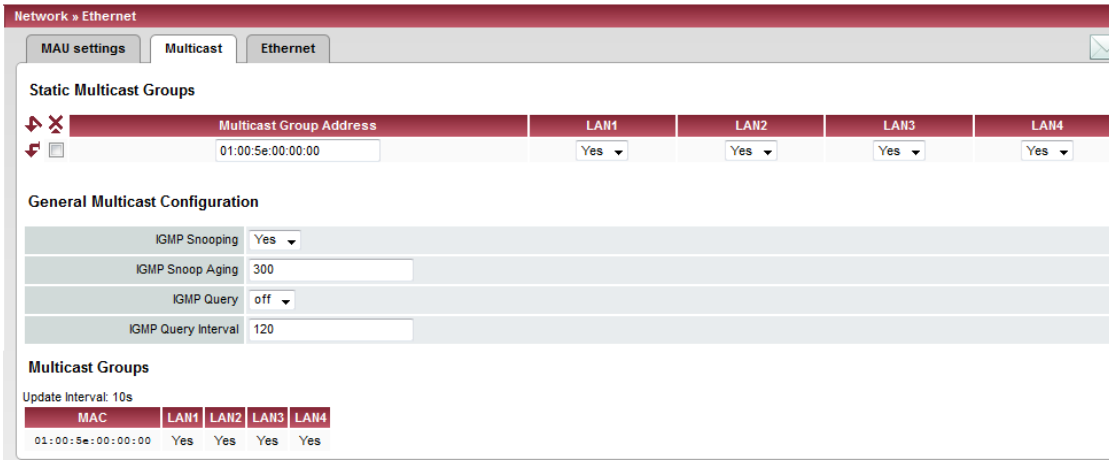
Network >> Ethernet >> MAU settings		
Port Mirroring Only for devices with an internal switch	**Port Mirroring Receiver**	The integrated switch controls port mirroring in order to monitor the network traffic. Here, you can decide which ports you want to monitor and the switch then sends copies of data packets from the monitored port to a selected port. The port mirroring function enables any packets to be forwarded to a specific recipient. You can select the receiver port or the mirroring of the incoming and outgoing packets from each switch port.
MAU Configuration	Configuration and status indication of the Ethernet connections:	
	Port	Name of the Ethernet connection to which the row refers.
	Media Type	Media type of the Ethernet connection.

Network >> Ethernet >> MAU settings [...]		
	Automatic Configuration	– **Yes**: tries to determine the required operating mode automatically. – **No**: uses the operating mode specified in the “Manual Configuration” column. When connecting the EAGLE mGuard to a hub, please note the following: when *Automatic Configuration* is deactivated, the Auto MDIX function is also deactivated. This means that the port of the EAGLE mGuard must either be connected to the uplink port of the hub or connected to the hub using a cross-link cable.
	Manual Configuration	The desired operating mode when *Automatic Configuration* is set to *No*.
	Current Mode	The current operating mode of the network connection.
	Port On	Switches the Ethernet connection on or off. The **Port On** function is **not** supported by mGuard centerport. The **Port On** function is supported with restrictions on: **mGuard delta**: the internal side (switch ports) cannot be switched off **mGuard pci**: in driver mode, the internal network interface cannot be switched off (however, this is possible in power-over-PCI mode)
	Port Mirroring	The port mirroring function enables any packets to be forwarded to a specific recipient. You can select the receiver port or the mirroring of the incoming and outgoing packets from each switch port.
	Link supervision	Only visible when the “Link supervision” menu item under Management >> Service I/O >> Alarm output is set to “Supervise”. If link supervision is active, the alarm output is opened if one link does not indicate connectivity.
Address Resolution Table Only for devices with an internal switch	**Port**	Name of the Ethernet connection to which the row refers.
	MACs	Lists the MAC addresses of the connected Ethernet-capable devices The switch can learn MAC addresses which belong to the ports of its connected Ethernet-capable devices. The contents of the list can be deleted by clicking the button.
Port Statistics Only for devices with an internal switch	A statistic is displayed for each physically accessible port of the integrated Managed Switch. The counter can be reset via the web interface or the following command: */Packages/mguard-api_0/mbin/action switch/reset-phy-counters*	
	Port	Name of the Ethernet connection to which the row refers.
	tx collisions	Number of errors while sending the data
	tx octets	Data volume sent

Network >> Ethernet >> MAU settings [...]		
	rx fcs errors	Number of received frames with invalid checksum
	rx good octets	Volume of the valid data received

6.2.2 Multicast

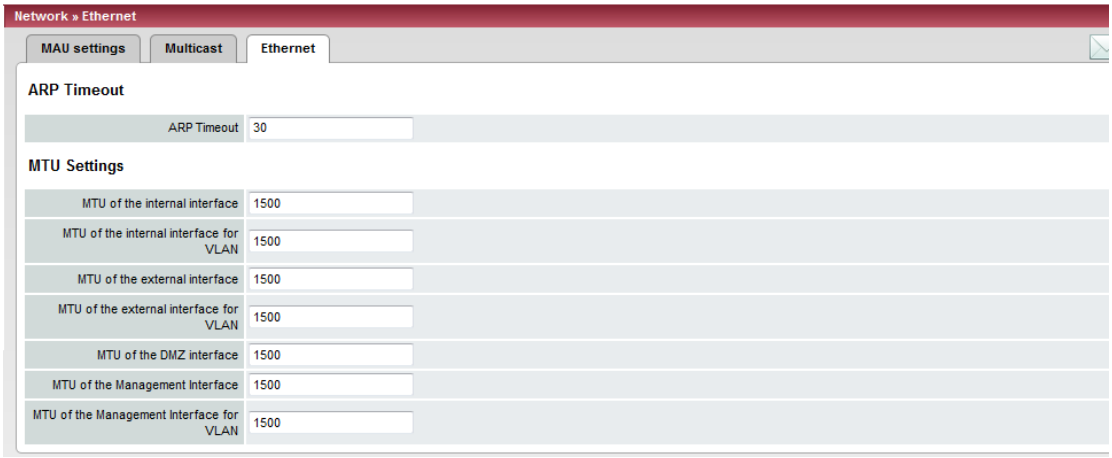
Only available with the mGuard rs4000 3G.



Network >> Ethernet >> Multicast		
Static Multicast Groups	Multicast is a technology which enables data to be sent to a group of recipients, without the transmitter having to send it multiple times. The data replication takes place through the distributor within the network. You can create a list of multicast addresses. The data is forwarded to the configured ports (LAN1 ... LAN4).	
General Multicast Configuration	**IGMP snooping**	The switch uses IGMP snooping to guarantee that multicast data is only forwarded via ports which are intended for this use.
	IGMP Snoop Aging	Period, after which membership to the multicast group expires, in seconds.
	IGMP Query	IGMP is used to join and leave a multicast group. Here, the IGMP version can be selected (V1 or V2, V3 is not supported)
	IGMP Query Interval	Interval in which IGMP queries are generated in seconds
Multicast Groups	**Displays the multicast groups. The display contains all static entries and the dynamic entries which are discovered by IGMP snooping.**	

6.2.3 Ethernet

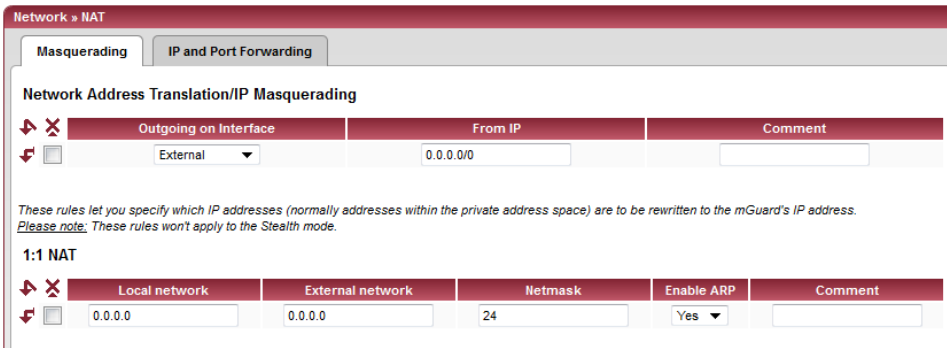
Only available with the mGuard rs4000 3G.



Network >> Ethernet >> Ethernet		
ARP Timeout	**ARP Timeout**	Service life (in seconds) of entries in the ARP table. MAC and IP addresses are assigned to each other in the ARP table.
MTU Settings	**MTU of the ... interface**	The maximum transfer unit (MTU) defines the maximum IP packet length that may be used for the relevant interface. For a VLAN interface: As VLAN packets contain 4 bytes more than those without VLAN, certain drivers may have problems processing these larger packets. Such problems can be solved by reducing the MTU to 1496.

6.3 Network >> NAT

6.3.1 Masquerading



Network >> NAT >> Masquerading

Masquerading (Network Address Translation/IP Masquerading)

Lists the rules established for NAT (**N**etwork **A**ddress **T**ranslation).

For outgoing data packets, the device can rewrite the specified sender IP addresses from its internal network to its own external address, a technique referred to as NAT (Network Address Translation), see also NAT (Network Address Translation) in the glossary.

This method is used if the internal addresses cannot or should not be routed externally, e.g., because a private address area such as 192.168.x.x or the internal network structure should be hidden.

The method can also be used to hide external network structures from the internal devices. To do so, set the **Internal** option under **Outgoing on Interface.** The **Internal** setting allows for communication between two separate IP networks where the IP devices have not configured a (useful) default route or differentiated routing settings (e.g., PLCs without the corresponding settings). The corresponding settings must be made under **1:1 NAT.**

This method is also referred to as *IP masquerading*.

Default settings: NAT is not active.

If the mGuard is operated in *PPPoE/PPTP* mode, NAT must be activated in order to gain access to the Internet. If NAT is not activated, only VPN connections can be used.

If multiple static IP addresses are used for the WAN port, the first IP address in the list is always used for IP masquerading.

These rules do not apply in Stealth mode.

Outgoing on Interface External/External 2/Any External[1]/Internal

Specifies via which interface the data packets are sent so that the rule applies to them. **Any External** refers to the **External** and **External 2** interfaces.

Network >> NAT >> Masquerading [...]

Masquerading is defined, which applies for network data flows in Router mode. These data flows are initiated so that they lead to a destination device which can be accessed over the selected network interface on the mGuard.

To do this, the mGuard replaces the IP address of the initiator with a suitable IP address of the selected network interface in all associated data packets. The effect is the same as for the other values of the same variables. The IP address of the initiator is hidden from the destination of the data flow. In particular, the destination does not require any routes in order to respond in a data flow of this type (not even a default route (default gateway)).

Set the firewall in order for the desired connections to be allowed. For incoming and outgoing rules, the source address must still correspond to the original sender if the firewall rules are used.

Please observe the outgoing rules when using the “External/External 2/Any External” settings (see “Outgoing rules” on page 208).

Please observe the incoming rules when using the “Internal” setting (see “Incoming rules” on page 206).

From IP — **0.0.0.0/0** means that all internal IP addresses are subject to the NAT procedure. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).

Comment — Can be filled with appropriate comments.

1:1 NAT

Lists the rules established for 1:1 NAT (Network Address Translation).

With 1:1 NAT, the sender IP addresses are exchanged so that each individual address is exchanged with another specific address, and is not exchanged with the same address for all data packets, as in IP masquerading. This enables the mGuard to mirror addresses from the internal network to the external network.

Example: The mGuard is connected to network 192.168.0.0/24 via its LAN port and to network 10.0.0.0/24 via its WAN port. By using 1:1 NAT, the LAN computer with IP address 192.168.0.8 can be accessed via IP address 10.0.0.8 in the external network.

The mGuard claims the IP addresses entered for the “External network” for the devices in its “Local network”. The mGuard returns ARP answers for all addresses from the specified “External network” on behalf of the devices in the “Local network”. Therefore, the IP addresses entered under “External network” must not be used. They must not be assigned to other devices or used in any way, as an IP address conflict would otherwise occur in the external network. This even applies when no device exists in the “Internal network” for one or more IP addresses from the specified “External network”.

Network >> NAT >> Masquerading [...]

Default settings: 1:1 NAT is not active.

1:1 NAT cannot be applied to the *External 2* interface.

1:1 NAT is only used in *Router* network mode.

Local network	The address of the network on the LAN port.
External network	The address of the network on the WAN port.
Netmask	The subnet mask as a value between 1 and 32 for the local and external network address (see also “CIDR (Classless Inter-Domain Routing)” on page 24).
Comment	Can be filled with appropriate comments.

[1] *External 2* and *Any External* are only for devices with a serial interface: *mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs, mGuard blade, mGuard delta[2], mGuard delta, EAGLE mGuard* (see “Secondary External Interface” on page 116).

6.3.2 IP and Port Forwarding

Network >> NAT >> IP and Port Forwarding

IP and Port Forwarding

Lists the rules defined for port forwarding (DNAT = Destination NAT).

Port forwarding performs the following: the headers of incoming data packets from the external network, which are addressed to the external IP address (or one of the external IP addresses) of the mGuard and to a specific port of the mGuard, are rewritten in order to forward them to a specific computer in the internal network and to a specific port on this computer. In other words, the IP address and port number in the header of incoming data packets are changed.

This method is also referred to as Destination NAT.

Port forwarding cannot be used for connections initiated via the *External 2*[1] interface.

[1] *External 2* is only for devices with a serial interface.

The rules defined here have priority over the settings made under Network Security >> Packet Filter >> Incoming Rules.

Protocol: TCP/UDP/GRE

Specify the protocol to which the rule should apply.

GRE

GRE protocol IP packets can be forwarded. However, only one GRE connection is supported at any given time. If more than one device sends GRE packets to the same external IP address, the mGuard may not be able to feed back reply packets correctly. We recommend only forwarding GRE packets from specific transmitters. These could be ones that have had a forwarding rule set up for their source address by entering the transmitter address in the “From IP” field, e.g., 193.194.195.196/32.

From IP

The sender address for forwarding.

0.0.0.0/0 means all addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).

From Port

The sender port for forwarding.

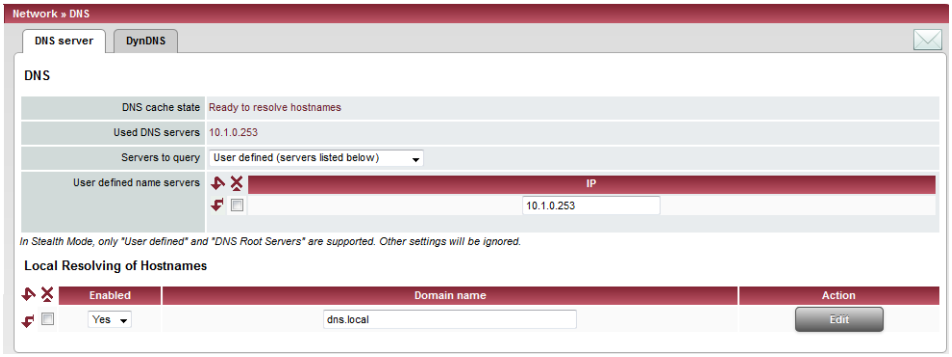
any refers to any port.

Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80.

Network >> NAT >> IP and Port Forwarding [...]	
Incoming on IP	– Specify the external IP address (or one of the external IP addresses) of the mGuard here, **or** – Use the variable **%extern** (if the external IP address of the mGuard is changed dynamically so that the external IP address cannot be specified). If multiple static IP addresses are used for the WAN port, the **%extern** variable always refers to the first IP address in the list.
Incoming on Port	The original destination port specified in the incoming data packets. Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80. This information is not relevant for the “GRE” protocol. It is ignored by the mGuard.
Redirect to IP	The internal IP address to which the data packets should be forwarded and into which the original destination addresses are translated.
Redirect to Port	The port to which the data packets should be forwarded and into which the original port data is translated. Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80. This information is not relevant for the “GRE” protocol. It is ignored by the mGuard.
Comment	Freely selectable comment for this rule.
Log	For each individual port forwarding rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default settings).

6.4 Network >> DNS

6.4.1 DNS server



Network >> DNS >> DNS server

DNS

If the mGuard is to initiate a connection to a partner on its own (e.g., to a VPN gateway or NTP server) and it is specified in the form of a host name (i.e., www.example.com), the mGuard must determine which IP address belongs to the host name. To do this, it connects to a domain name server (DNS) to query the corresponding IP address there. The IP address determined for the host name is stored in the cache so that it can be found directly (i.e., more quickly) for other host name resolutions.

With the *Local Resolving of Hostnames* function, the mGuard can also be configured to respond to DNS requests for locally used host names itself by accessing an internal, previously configured directory.

The locally connected clients can be configured (manually or via DHCP) so that the local address of the mGuard is used as the address of the DNS server to be used. If the mGuard is operated in *Stealth* mode, the management IP address of the mGuard (if this is configured) must be used for the clients, or the IP address 1.1.1.1 must be entered as the local address of the mGuard.

DNS cache state Status of the host name resolution

Used DNS servers DNS servers for which the associated IP address was queried.

Name servers to query

– **DNS Root Name Servers**

  Requests are sent to the root name servers on the Internet whose IP addresses are stored on the mGuard. These addresses rarely change.

– **Provider defined (e.g., via PPPoE or DHCP)**

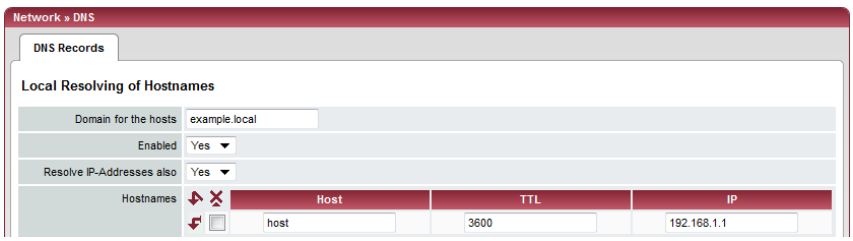
  The domain name servers of the Internet service provider that provide access to the Internet are used. Only select this setting if the mGuard operates in *PPPoE*, *PPTP*, *Modem* mode or in *Router* mode with DHCP.

– **User defined (from field below)**

  If this setting is selected, the mGuard will connect to the domain name servers listed under *User defined name servers*.

Network >> DNS >> DNS server [...]

	User defined name servers	The IP addresses of domain name servers can be entered in this list. If these should be used by the mGuard, select the “User defined (from field below)” option under **Servers to query**.
Local Resolving of Host-names	You can configure multiple entries with assignment pairs of host names and IP addresses for various domain names. You have the option to define, change (edit), and delete assignment pairs of host names and IP addresses. You can also activate or deactivate the resolution of host names for a domain. In addition, you can delete a domain with all its assignment pairs. Creating a table with assignment pairs for a domain: • Open a new row and click on **Edit** in this row. Changing or deleting assignment pairs belonging to a domain: • Click on **Edit** in the relevant table row. After clicking on **Edit**, the *DNS Records* tab page is displayed:	



Domain for the hosts	The name can be freely assigned, but it must adhere to the rules for assigning domain names. It is assigned to every host name.
Enabled	**Yes/No** Switches the *Local Resolving of Hostnames* function on (**Yes**) or off (**No**) for the domain specified in the field above.
Resolve IP-Addresses also	**No**: the mGuard only resolves host names, i.e., it supplies the assigned IP address for host names. **Yes**: same as for “No”. It is also possible to determine the host names assigned to an IP address.
Hostnames	The table can have any number of entries. A host name may be assigned to multiple IP addresses. Multiple host names may be assigned to one IP address.
TTL	Abbreviation for **T**ime **T**o **L**ive. Value specified in seconds. Default: 3600 (= 1 hour) Specifies how long called assignment pairs may be stored in the cache of the calling computer.
IP	The IP address assigned to the host name in this table row.

Example: Local Resolving of Hostnames

The “Local Resolving of Hostnames” function is used in the following scenario, for example:

A plant operates a number of identically structured machines, each one as a cell. The local networks of cells A, B, and C are each connected to the plant network via the Internet using the mGuard. Each cell contains multiple control elements, which can be addressed via their IP addresses. Different address areas are used for each cell.

A service technician should be able to use her/his notebook on site to connect to the local network for machine A, B or C and to communicate with the individual controllers. So that the technician does not have to know and enter the IP address for every single controller in machine A, B or C, host names are assigned to the IP addresses of the controllers in accordance with a standardized diagram that the service technician uses. The host names used for machines A, B, and C are identical, i.e., the controller for the packing machine in all three machines has the host name “pack”, for example. However, each machine is assigned an individual domain name, e.g., cell-a.example.com.

The service technician can connect her/his notebook to the local network at machine A, B or C and use the same host names in each of these networks to communicate with the corresponding machine controllers.

The notebook can obtain the IP address to be used, the name server, and the domain from the mGuard via DHCP.

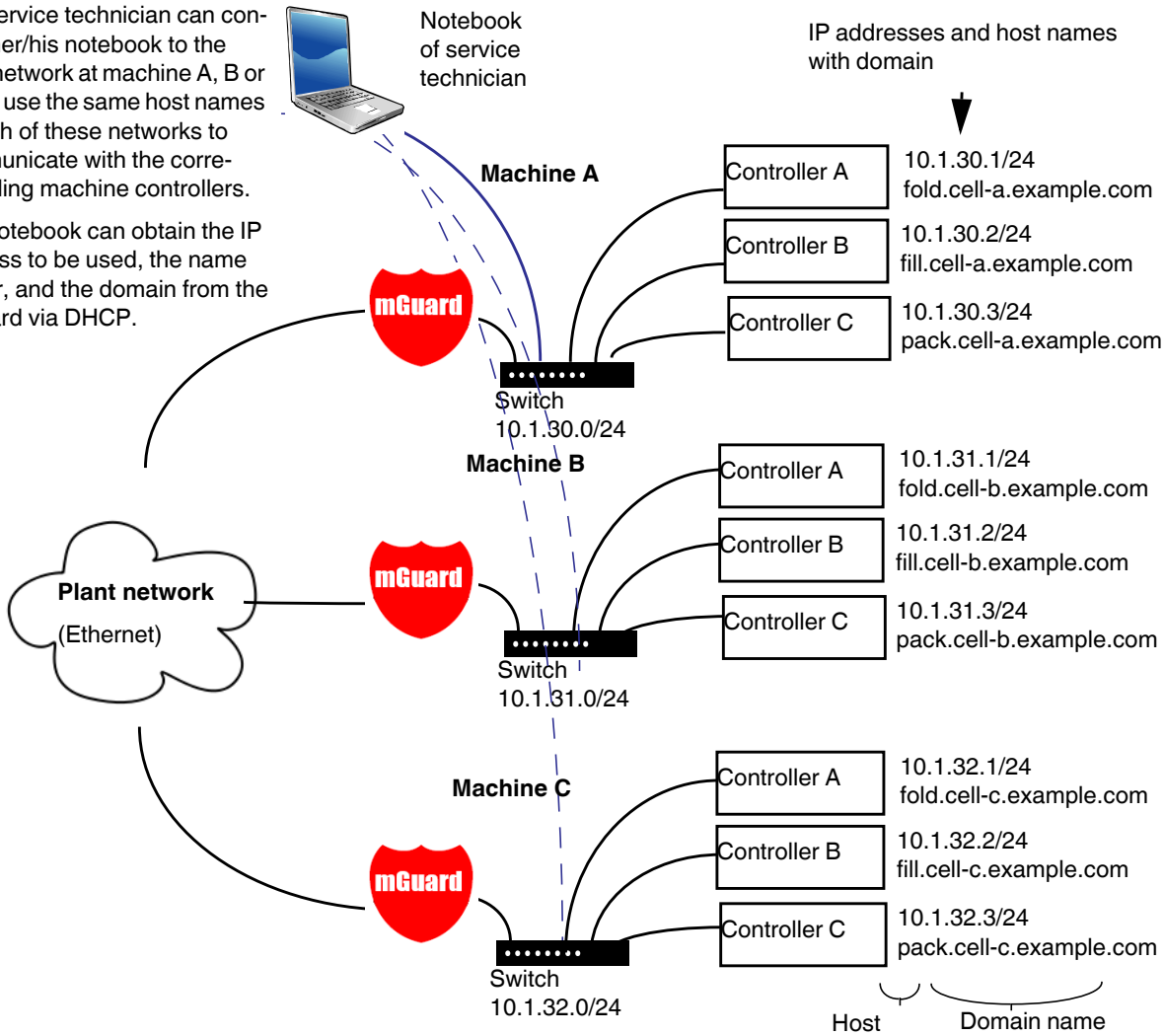
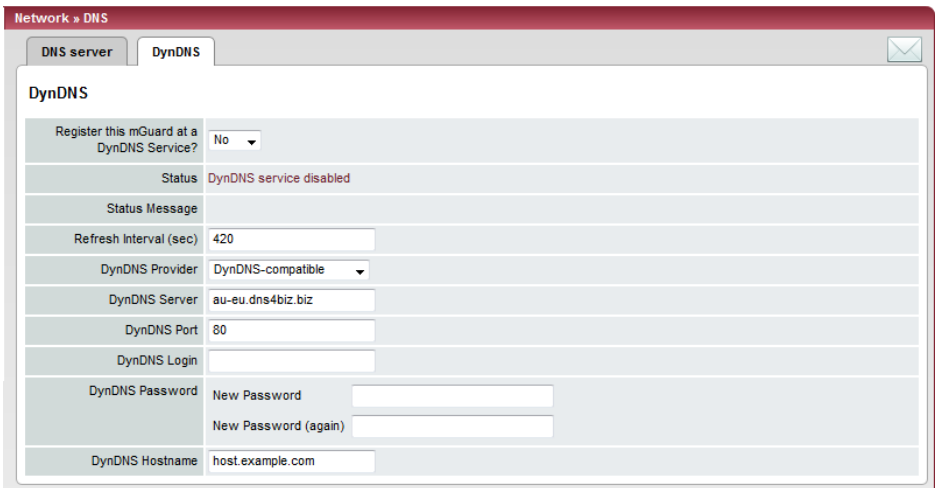


Figure 6-1 Local Resolving of Hostnames

6.4.2 DynDNS



Network >> DNS >> DynDNS

DynDNS

In order for a VPN connection to be established, at least one partner IP address must be known so that the partners can contact each other. This condition is not met if both participants are assigned IP addresses dynamically by their respective Internet service providers. In this case, a DynDNS service such as DynDNS.org or DNS4BIZ.com can be of assistance. With a DynDNS service, the currently valid IP address is registered under a fixed name.

If you have registered with one of the DynDNS services supported by mGuard, you can enter the corresponding information in this dialog box.

When using the mGuard rs4000/rs2000 3G, be aware that DynDNS is not permitted by all mobile network providers.

Register this mGuard at a DynDNS Service?

Select **Yes** if you have registered with a DynDNS provider and if the mGuard is to use this service. The mGuard then reports its current IP address to the DynDNS service (i.e., the one assigned for its Internet connection by the Internet service provider).

Refresh Interval (sec)

Default: 420 (seconds). The mGuard informs the DynDNS service of its new IP address whenever the IP address of its Internet connection is changed. In addition, the device can also report its IP address at the interval specified here. This setting has no effect for some DynDNS providers, such as DynDNS.org, as too many updates can cause the account to be closed.

DynDNS Provider

The providers in this list support the same protocol as the mGuard. Select the name of the provider with whom you are registered, e.g., DynDNS.org, TinyDynDNS, DNS4BIZ.

If your provider is not in the list, select **DynDNS-compatible** and enter the server and port for this provider.

DynDNS Server

Only visible when DynDNS Provider is set to **DynDNS-compatible**.

Name of the server for the DynDNS provider.

Network >> DNS >> DynDNS [...]		
	DynDNS Port	Only visible when DynDNS Provider is set to **DynDNS-compatible**. Name of the port for the DynDNS provider.
	DynDNS Login, DynDNS Password	Enter the user name and password assigned by the DynDNS provider here.
	DynDNS Hostname	The host name selected for this mGuard at the DynDNS service, providing you use a DynDNS service and have entered the corresponding data above. The mGuard can then be accessed via this host name.

6.5 Network >> DHCP

The Dynamic Host Configuration Protocol (DHCP) can be used to automatically assign the network configuration set here to the computer connected directly to the mGuard. Under *Internal DHCP* you can specify the DHCP settings for the internal interface (LAN port) and under External DHCP the DHCP settings for the external interface (WAN port). The “External DHCP” menu item is not included in the scope of functions for the mGuard rs2000.

The DHCP server also operates in *Stealth* mode.

In multi stealth mode, the external DHCP server of the mGuard cannot be used if a VLAN ID is assigned as the management IP.

IP configuration for Windows computers: when you start the DHCP server of the mGuard, you can configure the locally connected computers so that they obtain their IP addresses automatically.

Under Windows XP

- In the Start menu, select “Control Panel, Network Connections”.
- Right-click on the LAN adapter icon and select “Properties” from the context menu.
- On the “General” tab, select “Internet Protocol (TCP/IP)” under “This connection uses the following items”, then click on “Properties”.
- Make the appropriate entries and settings in the “Internet Protocol Properties (TCP/IP)” dialog box.

6.5.1 Internal/External DHCP

Network >> DHCP >> Internal DHCP

Mode

DHCP mode — **Disabled/Server/Relay**

Set this option to **Server** if the mGuard is to operate as an independent DHCP server. The corresponding setting options are then displayed below on the tab page (see “Server”).

Set this option to **Relay** if the mGuard is to forward DHCP requests to another DHCP server. The corresponding setting options are then displayed below on the tab page (see “Relay”).

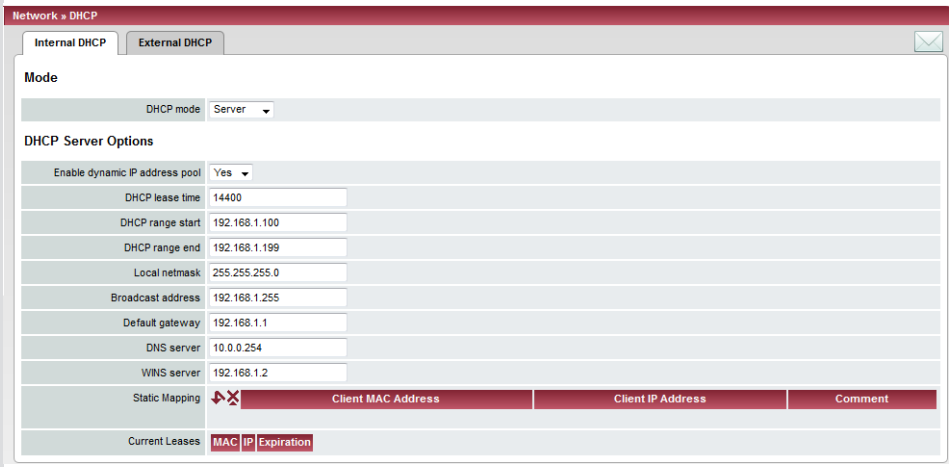
In mGuard *Stealth* mode, *Relay* DHCP mode is not supported. If the mGuard is in *Stealth* mode and *Relay* DHCP mode is selected, this setting will be ignored.

However, DHCP requests from the computer and the corresponding responses are forwarded due to the nature of Stealth mode.

If this option is set to **Disabled**, the mGuard does not answer any DHCP requests.

DHCP mode — **Server**

If DHCP mode is set to *Server*, the corresponding setting options are displayed below as follows.



Network >> DHCP >> Internal DHCP [...]		
DHCP Server Options	**Enable dynamic IP address pool**	Set this option to **Yes** if you want to use the IP address pool specified under *DHCP range start* and *DHCP range end* (see below). Set this option to “No” if only static assignments should be made using the MAC addresses (see below). **With enabled dynamic IP address pool:** When the DHCP server and the dynamic IP address pool have been activated, you can specify the network parameters to be used by the computer: **DHCP range start/end** The start and end of the address area from which the DHCP server of the mGuard should assign IP addresses to locally connected computers.
	DHCP lease time	Time in seconds for which the network configuration assigned to the computer is valid. The client should renew its assigned configuration shortly before this time expires. Otherwise it may be assigned to other computers.
	DHCP range start	**With enabled dynamic IP address pool** The start of the address area from which the DHCP server of the mGuard should assign IP addresses to locally connected computers.
	DHCP range end	**With enabled dynamic IP address pool** The end of the address area from which the DHCP server of the mGuard should assign IP addresses to locally connected computers.
	Local netmask	Specifies the subnet mask of the computers. Default: 255.255.255.0
	Broadcast address	Specifies the broadcast address of the computers.
	Default gateway	Specifies which IP address should be used by the computer as the default gateway. Usually this is the internal IP address of the mGuard.
	DNS server	Address of the server used by the computer to resolve host names in IP addresses via the Domain Name Service (DNS). If the DNS service of the mGuard is to be used, enter the internal IP address of the mGuard here.
	WINS server	Address of the server used by the computer to resolve host names in addresses via the Windows Internet Naming Service (WINS).

Network >> DHCP >> Internal DHCP [...]

Static Mapping [according to MAC address]

To find out the **MAC address** of your computer, proceed as follows:

Windows 95/98/ME:

- Start **winipcfg** in a DOS box.

Windows NT/2000/XP:

- Start **ipconfig /all** in a prompt. The MAC address is displayed as the “Physical Address”.

Linux:

- Call **/sbin/ifconfig** or **ip link show** in a shell.

The following options are available:

– Client/computer MAC address (without spaces or hyphens)

– Client's IP Address

Client IP Address

The static IP address of the computer to be assigned to the MAC address.

Static assignments take priority over the dynamic IP address pool.

Static assignments must not overlap with the dynamic IP address pool.

Do not use one IP address in multiple static assignments, otherwise this IP address will be assigned to multiple MAC addresses.

Only one DHCP server should be used per subnetwork.

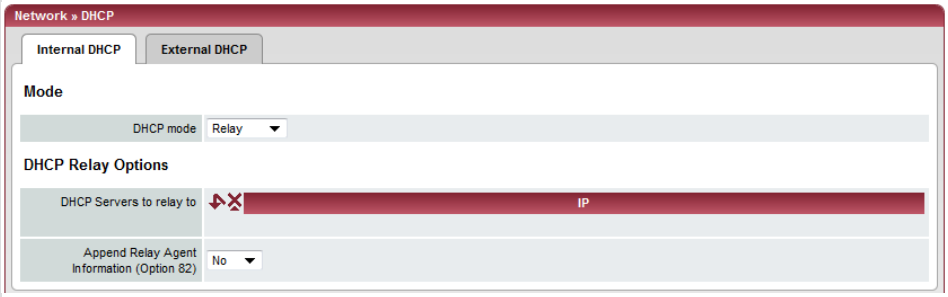
Current Leases

The current IP addresses (leases) for the internal and external DHCP servers assigned by the DHCP server are displayed with MAC address, IP address, and timeout.

Network >> DHCP >> Internal DHCP [...]

DHCP mode **Relay**

If DHCP mode is set to *Relay*, the corresponding setting options are displayed below as follows.



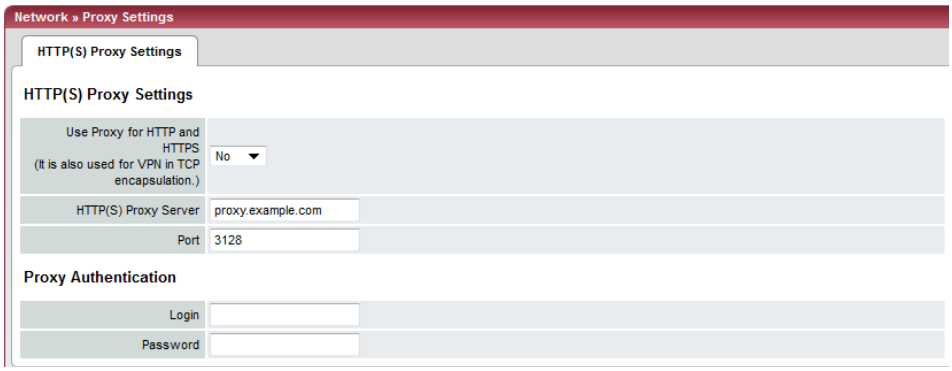
DHCP Relay Options

In mGuard *Stealth* mode, *Relay* DHCP mode is not supported. If the mGuard is in *Stealth* mode and *Relay* DHCP mode is selected, this setting will be ignored. However, DHCP requests from the computer and the corresponding responses are forwarded due to the nature of Stealth mode.

DHCP Servers to relay to	A list of one or more DHCP servers to which DHCP requests should be forwarded.
Append Relay Agent Information (Option 82)	When forwarding, additional information for the DHCP servers to which information is being forwarded can be appended according to RFC 3046.

6.6 Network >> Proxy Settings

6.6.1 HTTP(S) Proxy Settings



A proxy server can be specified here for the following activities performed by the mGuard itself:

– CRL download
– Firmware update
– Regular configuration profile retrieval from a central location
– Restoring of licenses

Network >> Proxy Settings >> HTTP(S) Proxy Settings		
HTTP(S) Proxy Settings	**Use Proxy for HTTP and HTTPS**	When set to **Yes**, connections that use the HTTP or HTTPS protocol are transmitted via a proxy server whose address and port should be specified in the next two fields.
	HTTP(S) Proxy Server	Host name or IP address of the proxy server.
	Port	Number of the port to be used, e.g., 3128.
Proxy Authentication	**Login**	User name for proxy server login.
	Password	Password for proxy server login.

6.7 Network >> Mobile Network

This menu is **only** available on the **mGuard rs4000/rs2000 3G.**

The **mGuard rs4000/rs2000 3G** supports the establishment of a WAN via mobile network. The following mobile network standards are supported.

- 3G/UMTS
- HSDPA+
- CDMA EV-DO
- EDGE
- GPRS

In addition, the GPS and GLONASS positioning systems are supported for positioning and time synchronization. Note that the time synchronization and position data from the positioning systems can be manipulated by interference signals (GPS spoofing).

Establishing a mobile network connection

To establish a mobile network connection, a matching **antenna** must be connected to the device (see device user documentation).

The mGuard also requires at least one valid **mini SIM card** in ID-000 format, via which it assigns and authenticates itself to a mobile network.

The mGuard rs4000/rs2000 3G can be equipped with two SIM cards. The SIM card in the SIM 1 slot is the primary SIM card which is normally used to establish the connection. If this connection fails, the device can turn to the second SIM card in slot SIM 2. You can set whether, and under which conditions, the connection to the primary SIM card is restored.

The state of the SIM cards is indicated via two LEDs on the front of the mGuard rs4000/rs2000 3G. The LEDs SIM1 and SIM2 light up green when the SIM card is active. If a PIN has not been entered, the LED flashes green.

Quality of the mobile network connection

The signal strength of the mobile network connection is indicated by three LEDs on the front of the mGuard rs4000/rs2000 3G. The LEDs function as a bar graph.

Table 6-1 LED indication of signal strength

LED 1 Lower LED	**LED 2** Middle LED	**LED 3** Upper LED	**Signal strength**	
Off	Off	Off	-113 dBm ... 111 dBm	Extremely poor to no network reception
Off	Off	Yellow	-109 dBm ... 89 dBm	Adequate network reception
Off	Green	Yellow	-87 dBm ... 67 dBm	Good network reception
Green	Green	Yellow	-65 dBm ... 51 dBm	Very good network reception

For stable data transmission, we recommend at least good network reception. If the network reception is only adequate, only text messages can be sent and received.

In the case of the **mGuard rs2000 3G**, the WAN is only available via the mobile network, as a WAN interface is not available. The mobile network function is preset. The mGuard rs2000 3G can only be operated in router mode.

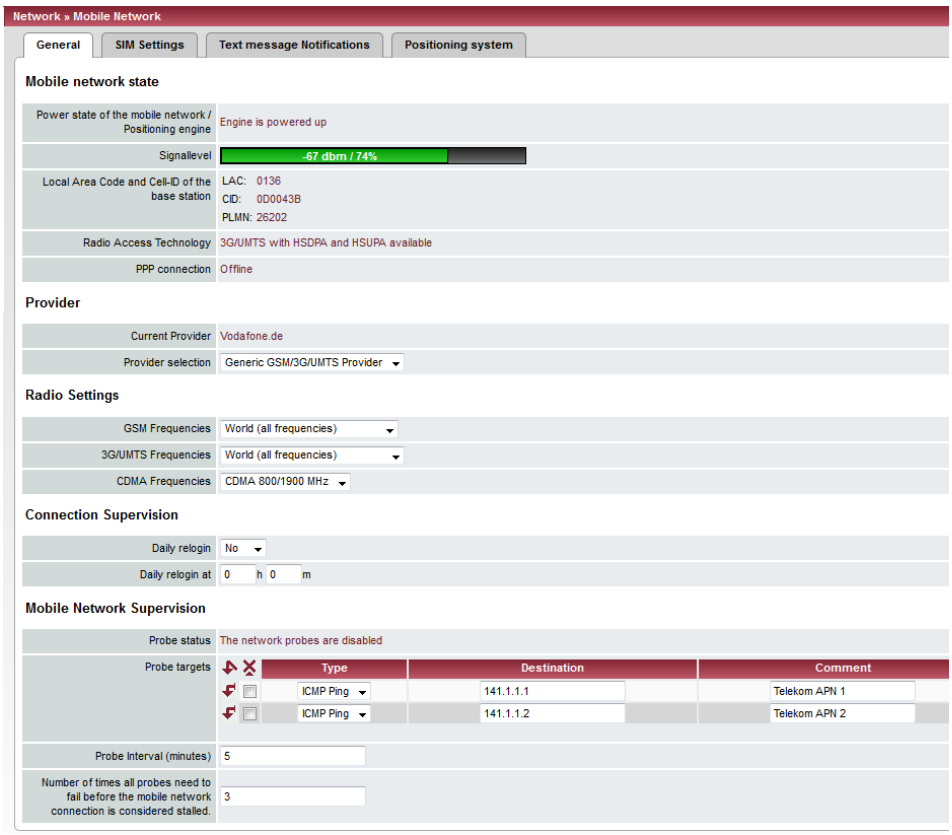
The status of the mobile network connection can be queried via SNMP. SNMP traps are sent in the following cases:

– Incoming text message
– Incoming call
– Mobile network connection error

You can switch SNMP support on and off under **Management >> SNMP.**

You can increase the amount of detail shown per entry in the log file of the mobile network connection. To do so, you need to set the “GSM_DEBUG” variable to “yes” via the console or SNMP.

6.7.1 General



Network >> Mobile Network >> General		
Mobile network state	**Power state of the mobile network / Positioning engine**	Indicates the state of the mobile network engine. **Engine is powered down** **Mobile network and positioning disabled:** mobile network and GPS switched off **Engine is powered up** **Only positioning possible:** mobile network disabled, GPS enabled **Mobile network connection for sending/receiving text message and calls, without packet data transmission:** SIM card inserted, PIN correctly entered **Mobile network connection for sending/receiving text message and calls, with packet data transmission:** – SIM card inserted – PIN correctly entered – Router network mode or secondary router mode set to “Built-in mobile network modem” – APN correctly entered – PPP authentication correctly stored
	Signal strength	Strength of the mobile network signal, from 0% ... 100%, -113 dBm ...>- 51 dBm The optimum received power is 100% signal strength and -51 dBm attenuation
	Local Area Code and Cell-ID of the base station	**LAC:** area code, location in mobile phone network **CID:** unique mobile phone cell ID **PLMN**: provider
	Radio Access Technology	GMS/EDGE/UTRAN/HSUPA/HSDPA/CDMA Shows the current mobile network standard.
	PPP connection	Shows the current status of the packet transmission.
Provider	**Current Provider**	Name of the mobile network provider
	Provider selection	**No mobile networking**: mobile network connection disabled **Generic GSM/UMTS Provider**: mobile network connection via the SIM card provider **Verizon CDMA (US)**: in the USA, mobile network connection without SIM card, via MEID code which is printed on the mGuard rs4000/rs2000 3G **AT&T 3G (US)**: in the USA, mobile network connection v ia AT&T

Network >> Mobile Network >> General [...]		
Radio settings	**GSM Frequencies**	Default: **World (all frequencies)** – GSM off – Europe/Asia (900/1800 MHz) – North America (850/1900 MHz) – Europe/Asia (900 MHz) – Europe/Asia (1800 MHz) – North America (850 MHz) – North America (1900 MHz)
	3G/UMTS Frequencies	Default: **World (all frequencies)** – UMTS off – World (850/1900/2100 MHz) – North America (850/1900 MHz) – Europe/Asia (2100 MHz) – Other countries (850/2100 MHz) – North America (850 MHz) – North America (1900 MHz) – World (800 MHz) – World (900 MHz)
	CDMA Frequencies	Default: **CDMA 800/1900 MHz** – CDMA off – CDMA 800 MHz – CDMA 1900 MHz – CDMA 800/1900 MHz
Connection Supervision	**Daily relogin**	The connection to the mobile network provider is renewed daily at a specified time. Otherwise, the mobile network operator regularly resets the connection from their side. Default: **No**
	Daily relogin at	Time at which the connection is renewed. The entry “Yes” must be selected under “Daily relogin” for this to take effect. For this to work correctly, the time must be successfully synchronized (realtime clock, NTP server, GPS/GLONASS) Default: **0 h : 0 m** Values: 0 – 23 hours and 0 – 59 minutes

Network >> Mobile Network >> General [...]	
Mobile Network Supervision	You can use the following probe targets to check whether data can actually be transmitted with an active mobile network connection with packet data transmission. To do so, probe targets (hosts) are pinged at specific intervals to see whether at least one of the targets can be reached. If the defined targets cannot be reached after specified intervals, the mobile network connection is reestablished. If SIM cards are available, the supervision runs as follows. – If a probe target was reached, the connection to the provider of the SIM 1 card is maintained. – If none of the probe targets could be reached, the connection switches to the provider of the other SIM card. – If the SIM 2 connection was active, it switches back to SIM 1. This ensures that SIM 1 is used primarily. The mobile network connection is also monitored. The mobile network modem is restarted if an AT command times out (timeout 30 seconds)
Probe status	Indicates whether supervision is activated. Supervision is only activated under the following conditions: – SIM card inserted – PIN correctly entered – Router mode or network mode set to “Built-in mobile network modem” – APN correctly entered – PPP authentication correctly stored

Network >> Mobile Network >> General [...]		
	Probe targets	Here you can enter the probe targets as host names or IP addresses. The ping type can be configured separately for each probe target: – ICMP Ping (ICMP echo request, ICMP echo reply) – DNS Ping (DNS query to UDP port 53) – IKE Ping (IPSec IKE query to UDP port 500) **Ping types** – IKE Ping: Determines whether a VPN gateway can be reached at the IP address specified. – ICMP Ping: Determines whether a device can be reached at the IP address specified. This is the most common ping test. However, the response to this ping test is disabled on some devices. This means that they do not respond even though they can be reached. – DNS Ping: Determines whether an operational DNS server can be reached at the IP address specified. A generic request is sent to the DNS server with the specified IP address, and every DNS server that can be reached responds to this request. The probe targets are processed in the specified order.
	Probe Interval	Indicates the time between two tests in minutes Value: 2 - 60 (default: 5)
	Number of times all probes need to fail before the mobile network connection is considered stalled	Number of repeats before the mobile network connection is considered to be aborted. Value: 1 - 5 (default: 3)

6.7.2 SIM Settings

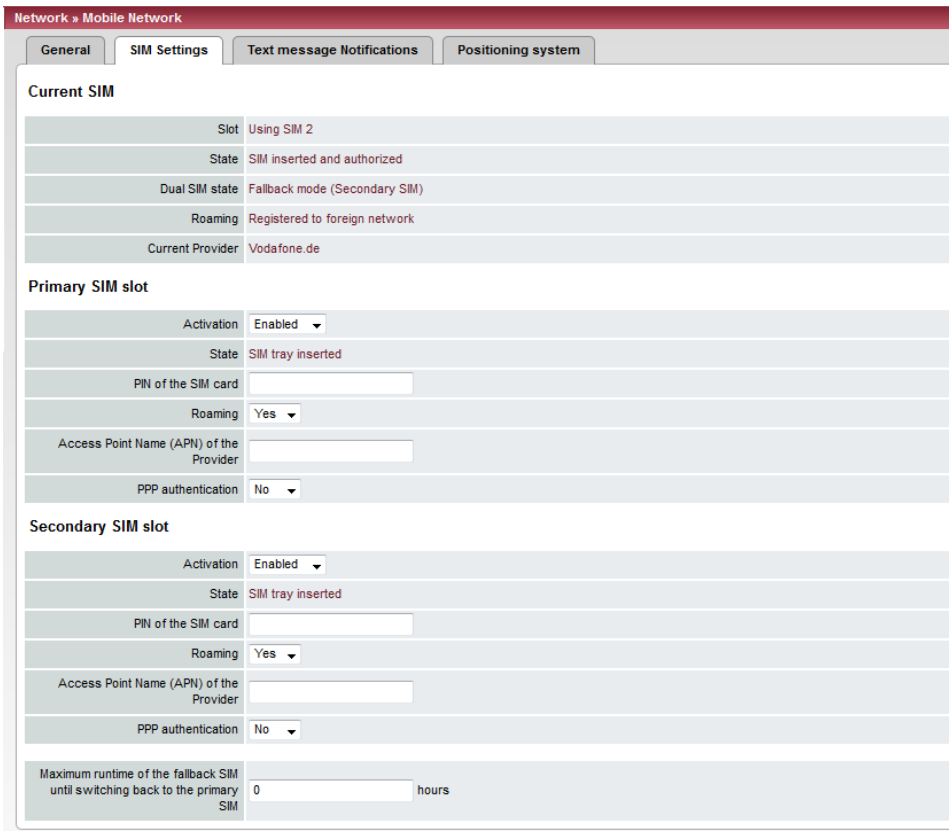
The mGuard rs4000/rs2000 3G can be equipped with two SIM cards. The SIM card in the SIM 1 slot is the primary SIM card which is normally used to establish the connection. If this connection fails, the device can turn to the second card in the SIM 2 slot.

The SIM card in slot 1 takes over the mobile network connection in these cases:

– If the mGuard is restarted
– When logging into the mobile network provider again
– In the event of an error with the mobile network connection of SIM 2
– If there is a timeout, which is set under “Maximum runtime of the fallback SIM until switching back to the primary SIM”

The SIM card in slot 2 takes over the mobile network connection if the connection via SIM 1 fails. The SIM card in slot 2 maintains the mobile network connection until one of the aforementioned cases occurs.

If SIM 2 is also unable to establish a mobile network connection, the intervals for successive logon attempts is increased to 60 seconds.



Network >> Mobile Network >> SIM Settings		
Current SIM	**Slot**	Indicates whether SIM 1 or SIM 2 is used.
	State	Indicates the state of the SIM card: – SIM state unknown – SIM inserted and authorized – Invalid SIM – SIM inserted No SIM found
	Roaming	If roaming is enabled, a mobile network device can also dial into another network. Here, the mobile network that the mGuard has dialed into is displayed. – **Not registered**: the mGuard has not dialed into any mobile network – **Registered to home network:** the mGuard has dialed into the mobile network provided – **Registered to foreign network**: the MGUARD has registered with a foreign mobile network
	Current Provider	Name of the mobile network provider in use
Primary SIM slot	**Activation**	You can prevent or enable the use of the SIM card.
	State	– SIM tray inserted (without SIM card) – No SIM tray (neither the SIM card nor tray are available) – Wrong PIN – PIN required – PUK required (if the pin is incorrectly entered too often) – SIM error (the SIM card could not be accessed) – SIM ready
	PIN of the SIM card	The SIM card can be protected with a PIN. The PIN is saved in the mGuard. The PIN is not displayed in the web browser. However, it is possible to overwrite or delete it. A PIN is used in the following cases: – When the mGuard is restarted – When the SIM card is replaced – When the PIN is changed – When the SIM card is activated – For login to a mobile network provider
	Roaming	Roaming enables or prevents dialing into foreign mobile networks. Dialing into another network can incur additional costs. When roaming is disabled, you can select a fixed provider.
	Provider selection	You can restrict the SIM card registration to a provider from the list. This selection is only active when roaming is disabled.

Network >> Mobile Network >> SIM Settings [...]		
	Access Point Name (APN) of the provider	Enter the name of the access gateway for the packet transmission of your mobile network provider. The APN can be obtained from your mobile network provider.
	PPP authentication	This is required by some providers for the transmission of packet data. The access data must be entered for this.
	PPP login name	Enter the PAP or CHAP user names to log on to the access gateway of the mobile network provider. This information can be obtained from your mobile network provider. Only visible when PPP authentication is set to “Yes”.
	PPP password	Enter the PAP or CHAP user password to log onto the access gateway of the mobile network provider. This information can be obtained from your mobile network provider. Only visible when PPP authentication is set to “Yes”.
Secondary SIM slot	**...**	See “Primary SIM slot”
	Maximum runtime of the fallback SIM until switching back to the primary SIM	Indicates the duration in hours until the device switches to back to SIM 1 from SIM 2. If set to “0”, SIM 2 remains active until the device dials into the mobile network again. Values: 0 – 24 hours.

6.7.3 Text message Notifications

The mGuard rs4000/rs2000 3G can send and receive text messages.

Text messages can be sent via the following mechanisms:

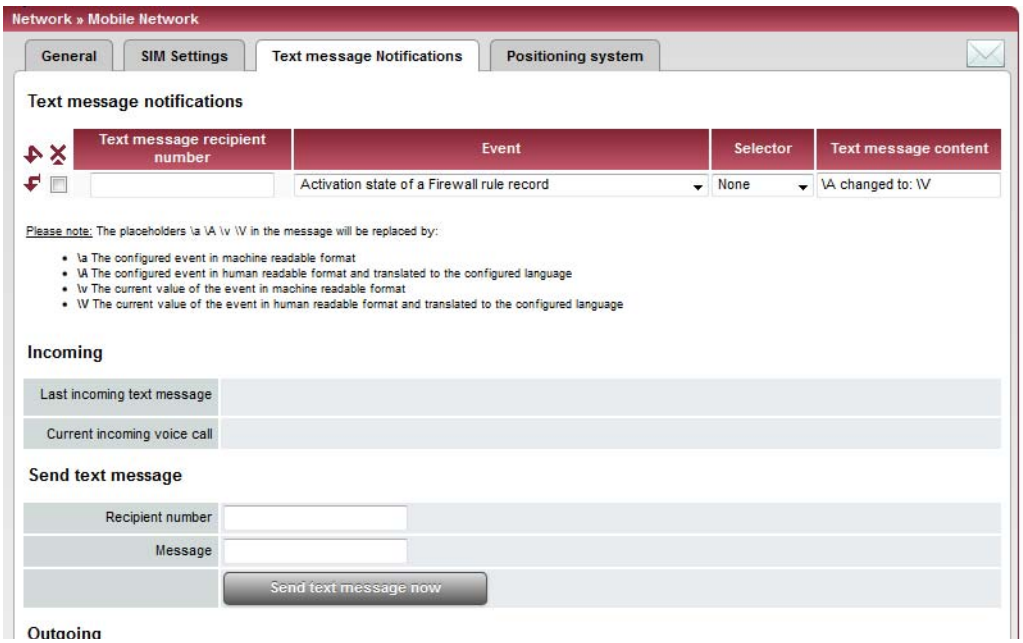
– Web interface
– Console

Text messages can be sent to freely definable mobile network recipients for selectable events. A complete list of all events can be found at “Event table” on page 53.

You can also send an text message via the console. To do so, you must enter the recipient number followed by a space and then add the message:

/Packages/mguard-api_0/mbin/action gsm/sms “<recipient number> <message>”

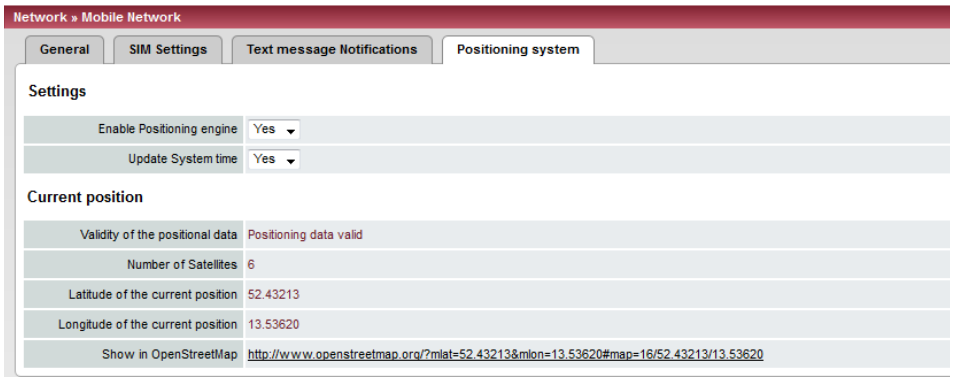
Incoming text messages can be used to control VPN connections.


Network » Mobile Network
General
SIM Settings
Text message Notifications
Positioning system
Text message notifications
Text message recipient number
Event
Selector
Text message content
Activation state of a Firewall rule record
None
\A changed to: \V
Please note: The placeholders \a \A \v \V in the message will be replaced by:
\a The configured event in machine readable format
\A The configured event in human readable format and translated to the configured language
\v The current value of the event in machine readable format
\V The current value of the event in human readable format and translated to the configured language
Incoming
Last incoming text message
Current incoming voice call
Send text message
Recipient number
Message
Send text message now
Outgoing

Network >> Mobile Network >> Text message Notifications		
Text message Notifications	Any text message recipient can be linked to predefined events and a freely definable message. The list is processed from top to bottom.	
	Text message recipient number	Defines a recipient number for the text message.
	Event	When the selected event occurs, the linked recipient number is selected and the event is sent to them as an text message. An text message can also be stored and sent. A complete list of all events can be found at “Event table” on page 53.

Network >> Mobile Network >> Text message Notifications [...]		
	Selector	A configured VPN connection can be selected here, which is monitored via text message.
	Text message content	Here you can enter the text that is sent as an text message. 160 characters maximum (7 bit ASCII, no umlauts, no special characters, no control characters) The text is freely definable. You can use blocks from the event table which can be inserted as wildcards in plain text (\A and \V) or in machine-readable form (\a and v\)
Incoming	Incoming text messages can be used to start or stop VPN connections. The text message must contain a preconfigured token and the corresponding command for the relevant VPN connection.	
	Text message command	vpn/start <token> vpn/stop <token> The token is defined in the VPN settings: “IPsec VPN >> Connections >> Edit >> General, Token for text message trigger”
	Last incoming text message	Displays the last text message received.
	Current incoming voice call	Displays the telephone number of the current incoming caller.
Send text message	**Recipient number**	Enter the telephone number of the recipient of the text message (22 characters maximum).
	Message	Here you can enter the text that is sent as an text message. 160 characters maximum (7 bit ASCII, no umlauts, no special characters, no control characters)
	Send text message now	The message is sent when you click the button.

6.7.4 Positioning system

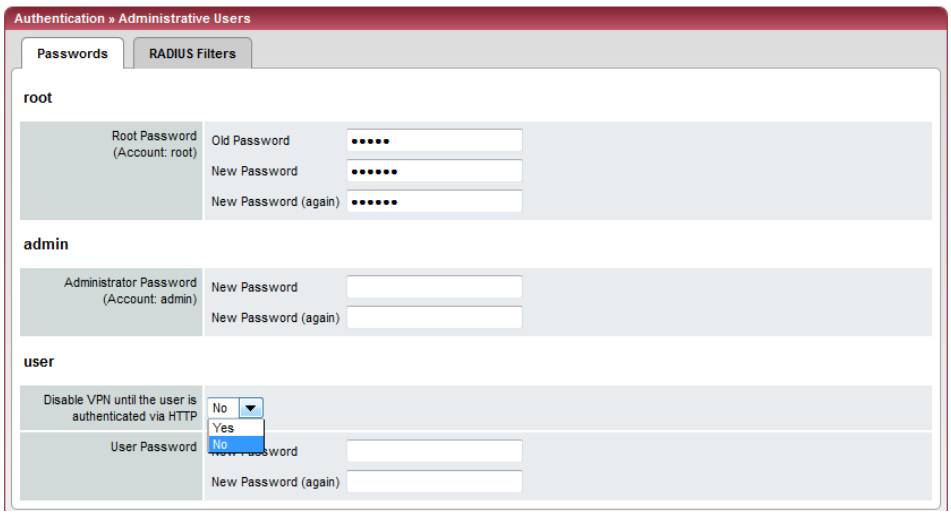


Network >> Mobile Network >> Positioning system		
Settings	**Enable positioning engine**	When you enable this function, the position of the mGuard is determined.
	Update System time	Enables time synchronization through the positioning system in use. When setting “Yes”, enter the local system time (under “Management >> System Settings >> Time and Date”).
Current position	**Validity of the positional data**	Indicates whether valid positioning data is available for the mGuard.
	Number of Satellites	Displays the number of available GPS/GLONASS satellites for the mGuard which are available for position determination. At least two satellites must be available. Four available satellites are required for precise position determination. The longitude and latitude can be precisely determined to 10 m. Values: 0 – 24
	Latitude of the current position	Displays the current latitude of the mGuard position.
	Longitude of the current position	Displays the current longitude of the mGuard position.
	Show in OpenStreetMap	When you enable this function, the position data of the mGuard is displayed. A functional Internet connection is required for this.

7 Authentication menu

7.1 Authentication >> Administrative Users

7.1.1 Passwords

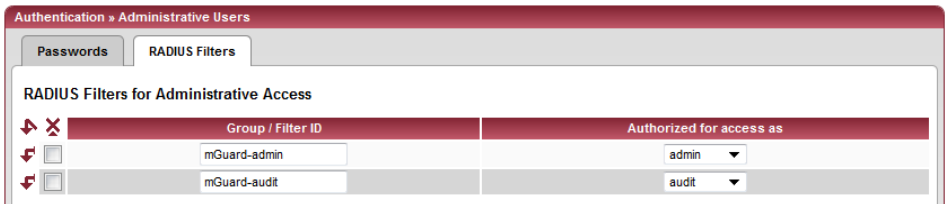


Administrative Users refers to users who have the right (depending on their authorization level) to configure the mGuard (*root* and *administrator* authorization levels) or to use it (*user* authorization level).

Authentication >> Administrative Users >> Passwords		
	To log into the corresponding authorization level, the user must enter the password assigned to the relevant authorization level (*root*, *admin* or *user*).	
root	**Root Password (Account: root)**	Grants full rights to all parameters of the mGuard. Background: only this authorization level allows unlimited access to the mGuard file system. User name (cannot be modified): **root** Default root password: **root** • To change the root password, enter the old password in the *Old Password* field, then the new password in the two corresponding fields below.
admin	**Administrator Password (Account: admin)**	Grants the rights required for the configuration options accessed via the web-based administrator interface. User name (cannot be modified): **admin** Default password: mGuard

Authentication >> Administrative Users >> Passwords [...]		
user	**Disable VPN until the user is authenticated via HTTP**	If a user password has been specified and activated, the user must always enter this password after an mGuard restart in order to **enable mGuard VPN connections** when attempting to access any HTTP URL. To use this option, specify the new user password in the corresponding entry field. This option is set to **No** by default. If set to **Yes**, VPN connections can only be used once a user has logged into the mGuard via HTTP. As long as authentication is required, all HTTP connections are redirected to the mGuard. Changes to this option only take effect after the next restart.
	User Password	There is no default user password. To set one, enter the desired password in both entry fields.

7.1.2 RADIUS Filters



Group names can be created here for administrative users whose password is checked using a RADIUS server when accessing the mGuard. Each of these groups can be assigned an administrative role.

Authentication >> Administrative Users >> RADIUS Filters

This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.

The mGuard only checks passwords using RADIUS servers if you have activated RADIUS authentication:

– For shell access, see menu: *Management >> System Settings >> Shell Access*
– For web access, see menu: *Management >> Web Settings >> Access*

The RADIUS filters are searched consecutively. When the first match is found, access is granted with the corresponding role (*admin*, *netadmin*, *audit*).

After a RADIUS server has checked and accepted a user's password, it sends the mGuard a list of filter IDs in its response.

These filter IDs are assigned to the user in a server database. They are used by the mGuard for assigning the group and hence the authorization level as “admin”, “netadmin” or “audit”.

If authentication is successful, this is noted as part of the mGuard's logging process. Other user actions are logged here using the original name of the user. The log messages are forwarded to a SysLog server, provided a SysLog server has been approved by the mGuard.

The following actions are recorded:

– Login
– Logout
– Start of a firmware update
– Changes to the configuration
– Password changes for one of the predefined users (*root, admin, netadmin, audit, and user*).

Authentication >> Administrative Users >> RADIUS Filters [...]		
RADIUS Filters for Administrative Access	**Group / Filter ID**	The group name may only be used once. Two lines must not have the same value. Answers from the RADIUS server with a notification of successful authentication must have this group name in their filter ID attribute. Up to 50 characters are allowed (printable UTF-8 characters only) without spaces.
	Authorized for access as	Each group is assigned an administrative role. **admin:** Administrator **netadmin**: Administrator for the network **audit**: Auditor The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager.

7.2 Authentication >> Firewall Users

To prevent private surfing on the Internet, for example, every outgoing connection is blocked under *Network Security >> Packet Filter >> DMZ*. VPN is not affected by this.

Under *Network Security >> User Firewall*, different firewall rules can be defined for certain users, e.g., outgoing connections are permitted. This user firewall rule takes effect as soon as the relevant firewall user(s) (to whom this user firewall rule applies) has (or have) logged in, see *"Network Security >> User Firewall" on page 225*.

7.2.1 Firewall Users

This menu is **not** available on the **mGuard rs2000 (3G)**.

Administrative access simultaneously via X.509 authentication and via login to the mGuard user firewall is not possible with the **Safari browser**.

Authentication >> Firewall Users >> Firewall Users		
Users	**Lists the firewall users by their assigned user names. Also specifies the authentication method.**	
	Enable user firewall	Under the *Network Security >> User Firewall* menu item, firewall rules can be defined and assigned to specific firewall users. When set to **Yes**, the firewall rules assigned to the listed users are applied as soon as the corresponding user logs in.
	Enable group authentication	If activated, the mGuard forwards login requests for unknown users to the RADIUS server. If successful, the response from the RADIUS server will contain a group name. The mGuard then enables user firewall templates containing this group name as the template user. The RADIUS server must be configured to deliver this group name in the "Access Accept" packet as a "Filter-ID=<group-name>" attribute.
	User Name	Name specified by the user during login.

Authentication >> Firewall Users >> Firewall Users[...]	
Authentication Method	**Local DB**: when *Local DB* is selected, the password assigned to the user must be entered in the *User Password* column in addition to the *User Name* that must be entered on login. **RADIUS**: if RADIUS is selected, the user password can be stored on the RADIUS server.
User Password	Only active if *Local DB* is selected as the authentication method.

7.2.2 Access

Authentication >> Firewall Users >> Access	
Authentication via HTTPS	**NOTE:** For authentication via an external interface, please consider the following: If a firewall user can log in via an “unsecure” interface and the user leaves the session without logging out correctly, the login session may remain open and could be misused by another unauthorized person. An interface is “unsecure”, for example, if a user logs in via the Internet from a location or a computer to which the IP address is assigned dynamically by the Internet service provider – this is usually the case for many Internet users. If such a connection is temporarily interrupted, e.g., because the user logged in is being assigned a different IP address, this user must log in again. However, the old login session under the old IP address remains open. This login session could then be used by an intruder, who uses this “old” IP address of the authorized user and accesses the mGuard using this sender address. The same thing could also occur if an (authorized) firewall user forgets to log out at the end of a session. This hazard of logging in via an “unsecure interface” is not completely eliminated, but the time is limited by setting the configured timeout for the user firewall template used. See “Timeout type” on page 227.

Authentication >> Firewall Users >> Access[...]	
Interface	**External/Internal/External 2/Dial-in[1]/DMZ[2]** Specifies which mGuard interfaces can be used by firewall users to log into the mGuard. For the interface selected, web access via HTTPS must be enabled: **Management**, **Web Settings** menu, *Access* tab page (see “Access” on page 57). In *Stealth* network mode, both the **Internal** and **External** interfaces must be enabled so that firewall users can log into the mGuard. (Two rows must be entered in the table for this.)

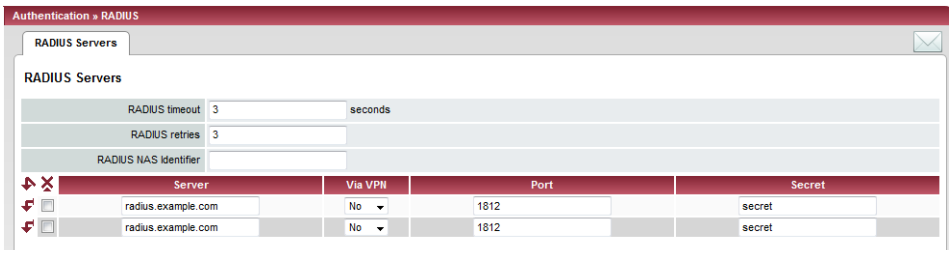
1 *External 2* and *Dial-in* are only for devices with a serial interface (see “Network >> Interfaces” on page 105).

2 *DMZ* is only for devices with a DMZ interface.

7.2.3 Status

When the user firewall is activated, its status is displayed here.

7.3 Authentication >> RADIUS



A RADIUS server is a central authentication server used by devices and services for checking user passwords. The password is not known to these devices and services. Only one or a number of RADIUS servers know the password.

The RADIUS server also provides the device or service that a user wishes to access with further information about the user, e.g., the group to which the user belongs. In this way, all user settings can be managed centrally.

In order to activate RADIUS authentication, **Yes** must be set under *Authentication* >> *Firewall Users (Enable group authentication* sub-item) and *RADIUS* selected as the *Authentication Method.*

Under Authentication >> RADIUS Servers, a list of RADIUS servers used by the mGuard is generated. This list is also used when RADIUS authentication is activated for administrative access (SSH/HTTPS).

When RADIUS authentication is active, the login attempt is forwarded from a non-predefined user (not: *root*, *admin*, *netadmin*, *audit* or *user*) to all RADIUS servers listed here. The first response received by the mGuard from one of the RADIUS servers determines whether or not the authentication attempt is successful.

Authentication >> RADIUS Servers

RADIUS servers

This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.

RADIUS timeout

Specifies the time (in seconds) the mGuard waits for a response from the RADIUS server. Default: 3 (seconds).

RADIUS retries

Specifies how often requests to the RADIUS server are repeated after the RADIUS timeout time has elapsed. Default: 3.

RADIUS NAS Identifier

A NAS ID (NAS identifier) is sent with every RADIUS request, except when the field remains empty.

All common characters on the keyboard (except for umlauts) can be used as the NAS ID.

The NAS ID is a RADIUS attribute that can be used by the client to be identified by the RADIUS server. The NAS ID can be used instead of an IP address to identify the client. It must be unique within the range of the RADIUS server.

Server

Name of the RADIUS server or its IP address.

We recommend entering IP addresses as servers instead of names, where possible. Otherwise, the mGuard must first resolve the names before it can send authentication queries to the RADIUS server. This takes time when logging in. Also, it may not always be possible to perform authentication if name resolution fails (e.g., because the DNS is not available or the name was deleted from the DNS).

Authentication >> RADIUS Servers [...]

Via VPN

If **Yes** is selected, the mGuard authentication query is always sent via an encrypted VPN tunnel if a suitable one is available.

If **No** is selected, a query of this type is always sent unencrypted outside the VPN.

If **Yes** has been selected under **Via VPN**, then the mGuard supports queries from a RADIUS server through its VPN connection. This happens automatically whenever the RADIUS server belongs to the remote network of a configured VPN tunnel and the mGuard has an internal IP address belonging to the local network of the same VPN tunnel. This makes the authentication query dependent on the availability of a VPN tunnel.

During configuration, ensure that the failure of a single VPN tunnel does not prevent administrative access to the mGuard.

Port

The port number used by the RADIUS server.

Secret

RADIUS server password.

This password must be the same as on the mGuard. The mGuard uses this password to exchange messages with the RADIUS server and to encrypt the user password. The RADIUS server password is not transmitted in the network.

The password is important for security since the mGuard can be rendered vulnerable to attack at this point if passwords are too weak. We recommend a password with at least 32 characters and several special characters. It must be changed on a regular basis.

If the RADIUS secret is discovered, an attacker can read the user password for the RADIUS authentication queries. An attacker can also falsify RADIUS responses and gain access to the mGuard if they know the user names. These user names are transmitted as plain text with the RADIUS request. The attacker can thus simulate RADIUS queries and thereby find out user names and the corresponding passwords.

Administrative access to the mGuard should remain possible while the RADIUS server password is being changed. Proceed as follows to ensure this:

- Set up the RADIUS server for the mGuard a second time with a new password.
- Also set this new password on the RADIUS server.
- On the mGuard, delete the line containing the old password.

7.4 Authentication >> Certificates

Authentication is a fundamental element of secure communication. The X.509 authentication method relies on certificates to ensure that the “correct” partners communicate with each other and that no “incorrect” partner is involved in communication. An “incorrect” communication partner is one who falsely identifies themselves as someone they are not (see glossary under “X.509 certificate” on page 363).

Certificate

A certificate is used as proof of the identity of the certificate owner. The relevant authorizing body in this case is the CA (certification authority). The digital signature on the certificate is provided by the CA. By providing this signature, the CA confirms that the authorized certificate owner possesses a private key that corresponds to the public key in the certificate.

The name of the certificate issuer appears under **Issuer** on the certificate, while the name of the certificate owner appears under *Subject*.

Self-signed certificates

A self-signed certificate is one that is signed by the certificate owner and not by a CA. In self-signed certificates, the name of the certificate owner appears under both **Issuer** and *Subject*.

Self-signed certificates are used if communication partners want to or must use the X.509 authentication method without having or using an official certificate. This type of authentication should only be used between communication partners that know and trust each other. Otherwise, from a security point of view, such certificates are as worthless as, for example, a home-made passport without the official stamp.

Certificates are shown to all communication partners (users or machines) during the connection process, providing the X.509 authentication method is used. In terms of the mGuard, this could apply to the following applications:

– Authentication of communication partners when establishing VPN connections (see “IPsec VPN >> Connections” on page 254, “Authentication” on page 269).
– Management of the mGuard via SSH (shell access) (see “Management >> System Settings >> Host” on page 33, “Shell Access” on page 40).
– Management of the mGuard via HTTPS (see “Management >> Web Settings” on page 56, “Access” on page 57).

Certificate, machine certificate

Certificates can be used to identify (authenticate) oneself to others. The certificate used by the mGuard to identify itself to others shall be referred to as the “machine certificate” here, in line with Microsoft Windows terminology.

A “certificate”, “certificate specific to an individual” or “user certificate showing a person” is one used by operators to authenticate themselves to partners (e.g., an operator attempting to access the mGuard via HTTPS and a web browser for the purpose of remote configuration). A certificate specific to an individual can also be saved on a chip card and then inserted by its owner in the card reader of their computer when prompted by a web browser during establishment of the connection, for example.

Remote certificate

A certificate is thus used by its owner (person or machine) as a form of ID in order to verify that they really are the individual they identify themselves as. As there are at least two communication partners, the process takes place alternately: partner A shows their certificate to partner B; partner B then shows their certificate to partner A.

Provision is made for the following so that A can accept the certificate shown by B, i.e., the certificate of its partner (thus allowing communication with B): A has previously received a copy of the certificate from B (e.g., by data carrier or e-mail) which B will use to identify itself to A. A can then verify that the certificate shown by B actually belongs to B by comparing it with this copy. With regard to the mGuard interface, the certificate copy given here by partner B to A is an example of a *remote certificate*.

For reciprocal authentication to take place, both partners must thus provide the other with a copy of their certificate in advance in order to identify themselves. A installs the copy of the certificate from B as its remote certificate. B then installs the copy of the certificate from A as its remote certificate.

Never provide the PKCS#12 file (file name extension: *.p12) as a copy of the certificate to the partner in order to use X.509 authentication for communication at a later time. The PKCS#12 file also contains the private key that must be kept secret and must not be given to a third party (see “Creation of certificates” on page 192).

To create a copy of a machine certificate imported in the mGuard, proceed as follows:

- On the “Machine Certificates” tab page, click on Current Certificate File next to the *Download Certificate* row for the relevant machine certificate (see “Machine Certificates” on page 197).

CA Certificates

The certificate shown by a partner can also be checked by the mGuard in a different way, i.e., not by consulting the locally installed remote certificate on the mGuard. To check the authenticity of possible partners in accordance with X.509, the method described below of consulting CA certificates can be used instead or as an additional measure, depending on the application.

CA certificates provide a way of checking whether the certificate shown by the partner is really signed by the CA specified in the partner's certificate.

A CA certificate is available as a file from the relevant CA (file name extension: *.cer, *.pem or *.crt). For example, this file may be available to download from the website of the relevant CA.

The mGuard can then check if the certificate shown by the partner is authentic using the CA certificates loaded on the mGuard. However, this requires all CA certificates to be made available to the mGuard in order to form a chain with the certificate shown by the partner. In addition to the CA certificate from the CA whose signature appears on the certificate shown by the partner to be checked, this also includes the CA certificate of the superordinate CA, and so forth, up to the root certificate (see glossary under “CA certificate” on page 357).

Authentication using CA certificates enables the number of possible partners to be extended without any increased management effort because it is not compulsory to install a remote certificate for each possible partner.

Creation of certificates

To create a certificate, a *private key* and the corresponding *public key* are required. Programs are available so that any user can create these keys. Similarly, a corresponding certificate with the corresponding *public key* can also be created, resulting in a self-signed certificate. (Additional information about self-creation can be downloaded from www.innominate.com. It is available in the download area in an application note entitled “How to obtain X.509 certificates”.)

A corresponding certificate signed by a CA must be requested from the CA.

In order for the private key to be imported into the mGuard with the corresponding certificate, these components must be packed into a PKCS#12 file (file name extension: *.p12).

Authentication methods

The mGuard uses two methods of X.509 authentication that are fundamentally different.

– The authentication of a partner is carried out based on the certificate and remote certificate. In this case, the remote certificate that is to be consulted must be specified for each individual connection, e.g., for VPN connections.
– The mGuard consults the CA certificates provided to check whether the certificate shown by the partner is authentic. This requires all CA certificates to be made available to the mGuard in order to form a chain with the certificate shown by the partner through to the root certificate.

“Available” means that the relevant CA certificates must be installed on the mGuard (see “CA Certificates” on page 199) and must also be referenced during the configuration of the relevant application (SSH, HTTPS, and VPN).

Whether both methods are used alternatively or in combination varies depending on the application (VPN, SSH, and HTTPS).

Restrictions using the Safari browser

Please note that during administrative access to the mGuard via an X.509 certificate using the **Safari browser** all sub-CA certificates must be installed in the browser's truststore.

Authentication for SSH

The partner shows the following:	Certificate (specific to individual), **signed by CA**	Certificate (specific to individual), **self-signed**
The mGuard authenticates the partner using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner PLUS (if required) Remote certificates, **if** used as a filter[1]	Remote certificate

1 (See “Management >> System Settings” on page 33, “Shell Access” on page 40)

Authentication for HTTPS

The partner shows the following:	Certificate (specific to individual), **signed by CA**[1]	Certificate (specific to individual), **self-signed**
The mGuard authenticates the partner using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner PLUS (if required) Remote certificates, **if** used as a filter[2]	Remote certificate

1 The partner can additionally provide sub-CA certificates. In this case, the mGuard can form the set union for creating the chain from the CA certificates provided and the self-configured CA certificates. The corresponding root CA certificate must always be available on the mGuard.

2 (See “Management >> Web Settings” on page 56, “Access” on page 57)

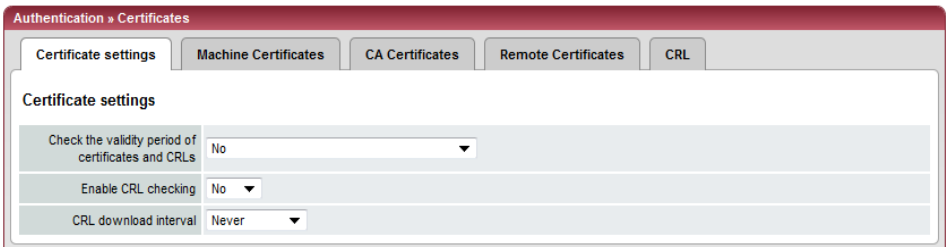
Authentication for VPN

The partner shows the following:	Machine certificate, **signed by CA**	Machine certificate, **self-signed**
The mGuard authenticates the partner using:		
	Remote certificate Or all CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner	Remote certificate

NOTE: It is not sufficient to simply install the certificates to be used on the mGuard under *Authentication* >> *Certificates*. In addition, the mGuard certificate imported from the pool that is to be used must be referenced in the relevant applications (VPN, SSH, HTTPS).

The remote certificate for authentication of a VPN connection (or the channels of a VPN connection) is installed in the *IPsec VPN* >> *Connections* menu.

7.4.1 Certificate settings



Authentication >> Certificates >> Certificate settings

Certificate settings

The settings made here relate to all certificates and certificate chains that are to be checked by the mGuard.

This generally excludes the following:

– Self-signed certificates from partners
– All remote certificates for VPN

Check the validity period of certificates and CRLs

No: the validity period specified in certificates and CRLs is ignored by the mGuard.

Wait for synchronization of the system time

The validity period specified in certificates and CRLs is only observed by the mGuard if the current date and time are known to the mGuard:

– Through the built-in clock (for the *mGuard rs4000/rs2000 3G*, *mGuard rs4000/rs2000*, *mGuard centerport, mGuard industrial rs*, *mGuard delta*, *mGuard smart*^{2}) or
– By synchronizing the system clock (see “Time and Date” on page 35)

Until this point, all certificates to be checked are considered invalid for security reasons.

Authentication >> Certificates >> Certificate settings[...]

Enable CRL checking

Yes: when CRL checking is enabled, the mGuard consults the CRL (certificate revocation list) and checks whether or not the certificates that are available to the mGuard are blocked.

CRLs are issued by the CAs and contain the serial numbers of blocked certificates, e.g., certificates that have been reported stolen.

On the **CRL** tab page (see “CRL” on page 203), specify the origin of the mGuard revocation lists....

When CRL checking is enabled, a CRL must be configured for each **issuer** of certificates on the mGuard. Missing CRLs result in certificates being considered invalid.

Revocation lists are verified by the mGuard using an appropriate CA certificate. Therefore, all CA certificates that belong to a revocation list (all sub-CA certificates and the root certificate) must be imported on the mGuard. If the validity of a revocation list cannot be proven, it is ignored by the mGuard.

If the use of revocation lists is activated together with the consideration of validity periods, revocation lists are ignored if (based on the system time) their validity has expired or has not yet started.

CRL download interval

If *Enable CRL checking* is set to **Yes** (see above), select the time period after which the revocation lists should be downloaded and applied.

On the **CRL** tab page (see “CRL” on page 203), specify the origin of the mGuard revocation lists.

If CRL checking is enabled, but CRL download is set to **Never**, the CRL must be manually loaded on the mGuard so that CRL checking can be performed.

7.4.2 Machine Certificates

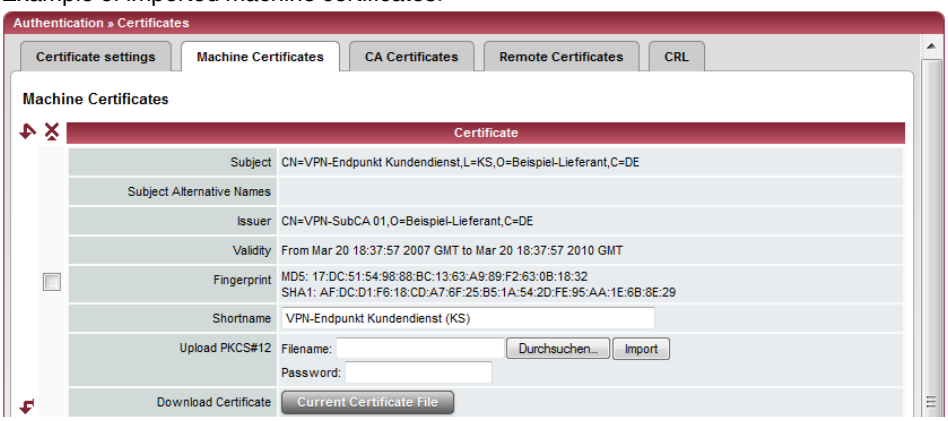
The mGuard authenticates itself to the partner using a machine certificate loaded on the mGuard. The machine certificate acts as an ID card for the mGuard, which it shows to the relevant partner.

For a more detailed explanation, see “Authentication >> Certificates” on page 190.

By importing a PKCS#12 file, the mGuard is provided with a private key and the corresponding machine certificate. Multiple PKCS#12 files can be loaded on the mGuard, enabling the mGuard to show the desired self-signed or CA-signed machine certificate to the partner for various connections.

In order to use the machine certificate installed at this point, it must be referenced **additionally** during the configuration of applications (SSH, VPN) so that it can be used for the relevant connection or remote access type.

Example of imported machine certificates:



Authentication >> Certificates >> Machine Certificates	
Machine Certificates	**Shows the currently imported X.509 certificates that the mGuard uses to authenticate itself to partners, e.g., other VPN gateways.**

To import a (new) certificate, proceed as follows:

Importing a new machine certificate

Requirement:

The PKCS#12 file (file name extension: *.p12 or *.pfx) is saved on the connected computer.

Proceed as follows:

- Click on **Browse...** to select the file.
- In the *Password* field, enter the password used to protect the private key of the PKCS#12 file.
- Click on **Import**.

  Once imported, the loaded certificate appears under *Certificate*.
- Remember to save the imported certificate along with the other entries by clicking on the **Apply** button.

Shortname

When importing a machine certificate, the CN attribute from the certificate subject field is suggested as the short name here (providing the *Shortname* field is empty at this point). This name can be adopted or another name can be chosen.

- A name must be assigned, whether it is the suggested one or another. Names must be unique and must not be assigned more than once.

Using the short name:

During the configuration of

– SSH (*Management* >> *System Settings, Shell Access* menu)
– HTTPS (*Management* >> *Web Settings, Access* menu)
– VPN connections (*IPsec VPN* >> *Connections* menu)

the certificates imported on the mGuard are provided in a selection list.

The certificates are displayed under the short name specified for each individual certificate on this page.

For this reason, name assignment is mandatory.

Creating a certificate copy

You can create a copy of the imported machine certificate (e.g., for the partner in order to authenticate the mGuard). This copy does not contain the private key and can therefore be made public at any time.

To do this, proceed as follows:

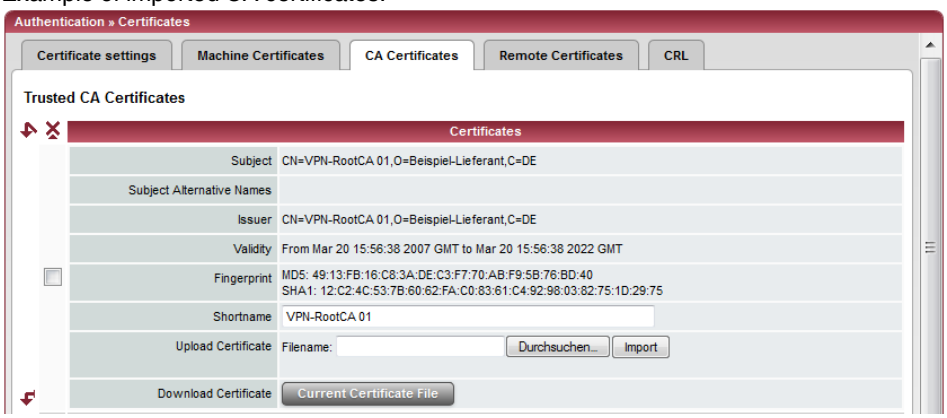
- Click on Current Certificate File next to the *Download Certificate* row for the relevant machine certificate.
- Enter the desired information in the dialog box that opens.

7.4.3 CA Certificates

CA certificates are certificates issued by a certification authority (CA). CA certificates are used to check whether the certificates shown by partners are authentic.

The checking process is as follows: the certificate issuer (CA) is specified as the issuer in the certificate transmitted by the partner. These details can be verified by the same issuer using the local CA certificate. For a more detailed explanation, see “Authentication >> Certificates” on page 190.

Example of imported CA certificates:



Authentication >> Certificates >> CA Certificates

Trusted CA Certificates — **Displays the current imported CA certificates.**

To import a (new) certificate, proceed as follows:

Importing a CA certificate

The file (file name extension: *.cer, *.pem or *.crt) is saved on the connected computer.

Proceed as follows:

- Click on **Browse...** to select the file.
- Click on **Import**. Once imported, the loaded certificate appears under *Certificate*.
- Save the imported certificate by clicking on **Apply**.

Shortname

When importing a CA certificate, the CN attribute from the certificate subject field is suggested as the short name here (providing the Shortname field is empty at this point). This name can be adopted or another name can be chosen.

- You must assign a name. The name must be unique.

Using the short name

During the configuration of

– SSH (*Management* >> *System Settings, Shell Access* menu)
– HTTPS (*Management* >> *Web Settings, Access* menu)
– VPN connections (*IPsec VPN* >> *Connections* menu)

the certificates imported on the mGuard are provided in a selection list. The certificates are displayed under the short name specified for each certificate in this selection list. Name assignment is mandatory.

Creating a certificate copy

A copy can be created from the imported CA certificate.

To do this, proceed as follows:

• Click on Current Certificate File next to the *Download Certificate* row for the relevant CA certificate. A dialog box opens in which you can enter the required information.

7.4.4 Remote Certificates

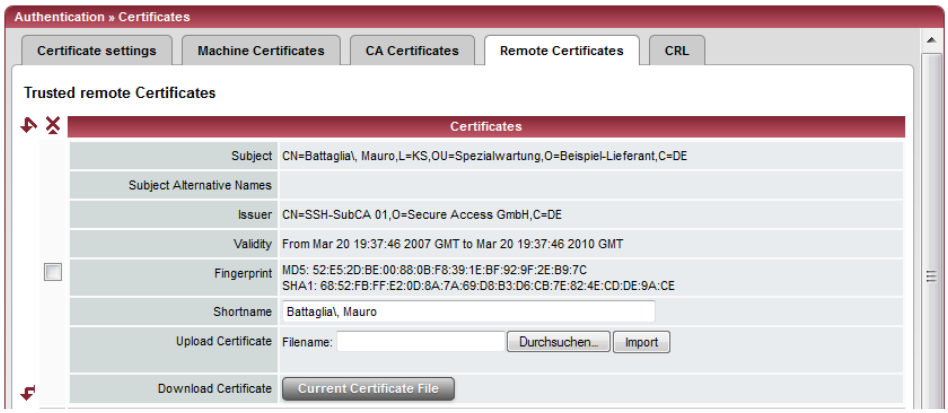
A remote certificate is a copy of the certificate that is used by a partner to authenticate itself to the mGuard.

Remote certificates are files (file name extension: *.cer, *.pem or *.crt) received from possible partners by trustworthy means. You load these files on the mGuard so that reciprocal authentication can take place. The remote certificates of several possible partners can be loaded.

The remote certificate for authentication of a VPN connection (or the channels of a VPN connection) is installed in the *IPsec VPN >> Connections* menu.

For a more detailed explanation, see “Authentication >> Certificates” on page 190.

Example of imported remote certificates:



Authentication >> Certificates >> Remote Certificates	
Trusted remote Certificates	**Displays the current imported remote certificates.**

Importing a new certificate

Requirement:

The file (file name extension: *.cer, *.pem or *.crt) is saved on the connected computer.

Proceed as follows:

- Click on **Browse...** to select the file.
- Click on **Import**.

  Once imported, the loaded certificate appears under *Certificate*.
- Remember to save the imported certificate along with the other entries by clicking on the **Apply** button.

Shortname

When importing a remote certificate, the CN attribute from the certificate subject field is suggested as the short name here (providing the *Shortname* field is empty at this point). This name can be adopted or another name can be chosen.

- A name must be assigned, whether it is the suggested one or another. Names must be unique and must not be assigned more than once.

Using the short name:

During the configuration of

– SSH (*Management >> System Settings, Shell Access* menu)
– HTTPS (*Management >> Web Settings, Access* menu)

the certificates imported on the mGuard are provided in a selection list. The certificates are displayed under the short name specified for each certificate in this selection list. Name assignment is mandatory.

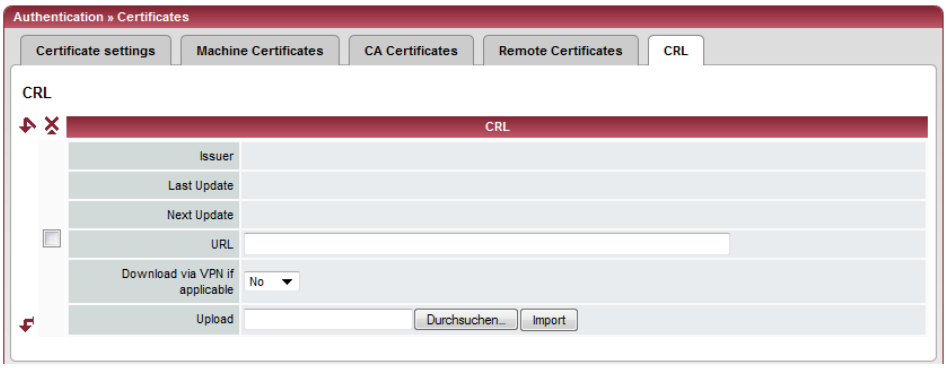
Creating a certificate copy

A copy can be created from the imported remote certificate.

To do this, proceed as follows:

• Click on Current Certificate File next to the *Download Certificate* row for the relevant remote certificate. A dialog box opens in which you can enter the required information.

7.4.5 CRL



Authentication >> Certificates >> CRL	
CRL	CRL stands for certificate revocation list. The CRL is a list containing serial numbers of blocked certificates. This page is used for the configuration of sites from which the mGuard should download CRLs in order to use them. Certificates are only checked for revocations if the **Enable CRL checking** option is set to **Yes** (see “Certificate settings” on page 195). A CRL with the same **issuer** name must be present for each **issuer** name specified in the certificates to be checked. If such a CRL is not present and CRL checking is enabled, the certificate is considered invalid.
Issuer	Information read directly from the CRL by the mGuard: Shows the issuer of the relevant CRL.
Last Update	Information read directly from the CRL by the mGuard: Time and date of issue of the current CRL on the mGuard.
Next Update	Information read directly from the CRL by the mGuard: Time and date when the CA will next issue a new CRL. This information is not influenced or considered by the CRL download interval.
URL	Specify the URL of the CA where CRL downloads are obtained if the CRL should be downloaded on a regular basis, as defined under CRL download interval on the *Certificate settings* tab page (see “Certificate settings” on page 195).
Download via VPN if applicable	If set to **Yes**, the mGuard uses a VPN tunnel to access the URL where the CRL is available for download. For this to happen, a suitable VPN tunnel must be configured, activated, and allow access. Otherwise, the CRL downloads from this URL will not be forwarded via a VPN tunnel.

Authentication >> Certificates >> CRL		
	Upload	If the CRL is available as a file, it can also be loaded on the mGuard manually. • To do this, click on **Browse...**, select the file, and click on **Import**. • Remember to save the imported CRL along with the other entries by clicking on the “Apply” button. An up-to-date CRL file must always be used. For this reason, it is not included in the mGuard configuration. When exporting an mGuard configuration and then importing it to another mGuard, the CRL file must be uploaded again. CRL files might be deleted during a firmware update. In this case, the mGuard downloads the CRL files from the specified URL again. Alternatively, it can be uploaded manually.

8 Network Security menu

This menu is **not** available on the **mGuard blade controller**.
A reduced version of the menu is available on the **mGuard rs2000 (3G)**.

8.1 Network Security >> Packet Filter

The mGuard includes a *Stateful Packet Inspection Firewall*. The connection data of an active connection is recorded in a database (connection tracking). Rules can thus only be defined for one direction. This means that data from the other direction of the relevant connection, and only this data, is automatically allowed through.

A side effect is that existing connections are not aborted during reconfiguration, even if a corresponding new connection can no longer be established.

Default firewall settings

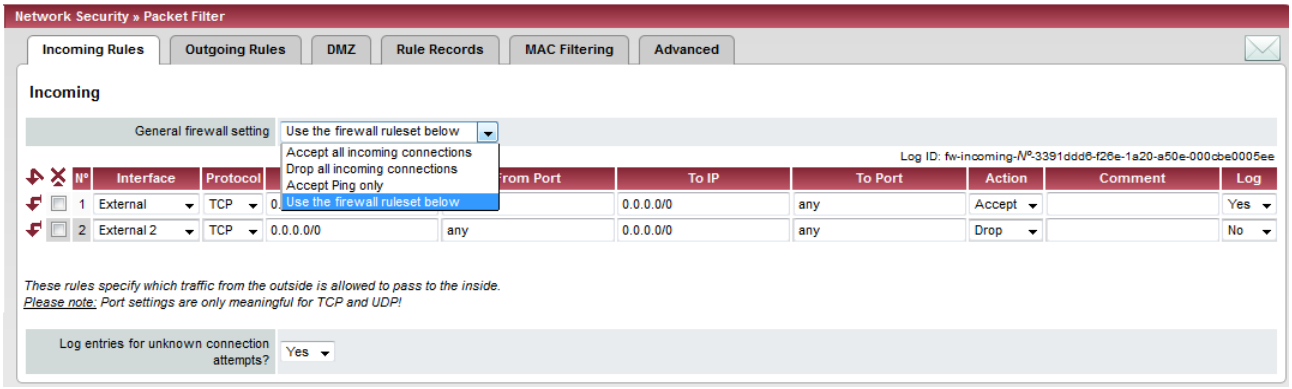
– All incoming connections are rejected (excluding VPN).
– Data packets of all outgoing connections are allowed through.

The firewall rules here have an effect on the firewall that is permanently active, with the exception of:

– **VPN connections**. Individual firewall rules are defined for VPN connections (see “IPsec VPN >> Connections” on page 254, “Firewall” on page 276).
– **User firewall**. When a user logs in, for whom user firewall rules are defined, these rules take priority (see “Network Security >> User Firewall” on page 225), followed by the permanently active firewall rules.

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied.
If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

8.1.1 Incoming rules



Network Security >> Packet Filter >> Incoming Rules

Incoming

Lists the firewall rules that have been set up. They apply for incoming data links that have been initiated externally.

If no rule has been set, the data packets of all incoming connections (excluding VPN) are dropped (default settings).

General firewall setting

Accept all incoming connections: the data packets of all incoming connections are allowed.

Drop all incoming connections: the data packets of all incoming connections are discarded.

Accept Ping only: the data packets of all incoming connections are discarded, except for ping packets (ICMP). This setting allows all ping packets to pass. The integrated protection against brute force attacks is not effective in this case.

Use the firewall ruleset below: displays further setting options. (This menu item is not included in the scope of functions for the mGuard rs2000 3G and mGuard rs2000).

The following settings are only visible if "**Use the firewall ruleset below**" is set.

Interface

External/External 2/Any External[1]

Specifies via which interface the data packets are received so that the rule applies to them. **Any External** refers to the **External** and **External 2** interfaces. These interfaces are only available on mGuard models that have a serial interface with external access.

Protocol

All means TCP, UDP, ICMP, GRE, and other IP protocols

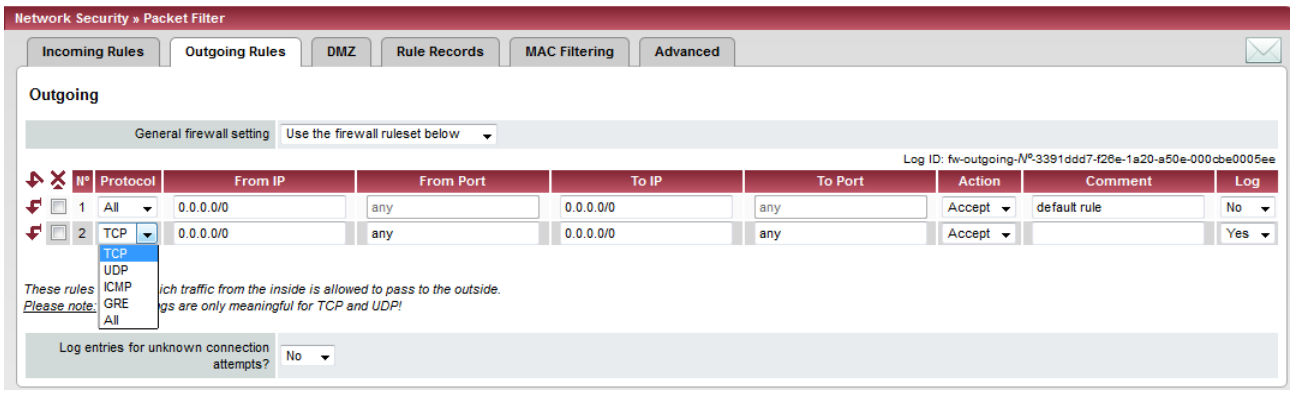
From IP/To IP

0.0.0.0/0 means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 24).

Network Security >> Packet Filter >> Incoming Rules[...]	
From Port/To Port	(Only evaluated for TCP and UDP protocols.) – **any** refers to any port. – **startport:endport** (e.g., 110:120) refers to a port area. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. In Stealth mode, **Reject** has the same effect as **Drop**. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule sets**, if defined. When a name is specified for rule sets, the firewall rules saved under this name take effect (see *Rule Records* tab page).
Comment	Freely selectable comment for this rule.
Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default settings).
Log entries for unknown connection attempts	When set to **Yes**, all connection attempts that are not covered by the rules defined above are logged. (Default settings: **No**)

[1] *External 2* and *Any External* are only for devices with a serial interface (see “Network >> Interfaces” on page 105).

8.1.2 Outgoing rules



Network Security >> Packet Filter >> Outgoing Rules

Outgoing

Lists the firewall rules that have been set up. They apply for outgoing data links that have been initiated internally in order to communicate with a remote partner.

Default setting: a rule is defined by default that allows all outgoing connections.

If no rule is defined, all outgoing connections are prohibited (excluding VPN).

General firewall setting

Allow all outgoing connections: the data packets of all outgoing connections are allowed.

Drop all outgoing connections: the data packets of all outgoing connections are discarded.

Accept Ping only: the data packets of all outgoing connections are discarded, except for ping packets (ICMP).

Use the firewall ruleset below: displays further setting options. (This menu item is not included in the scope of functions for the mGuard rs2000 3G and mGuard rs2000).

The following settings are only visible if "**Use the firewall ruleset below**" is set.

Protocol

All means TCP, UDP, ICMP, GRE, and other IP protocols

From IP/To IP

0.0.0.0/0 means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 24).

From Port/To Port

(Only evaluated for TCP and UDP protocols.)

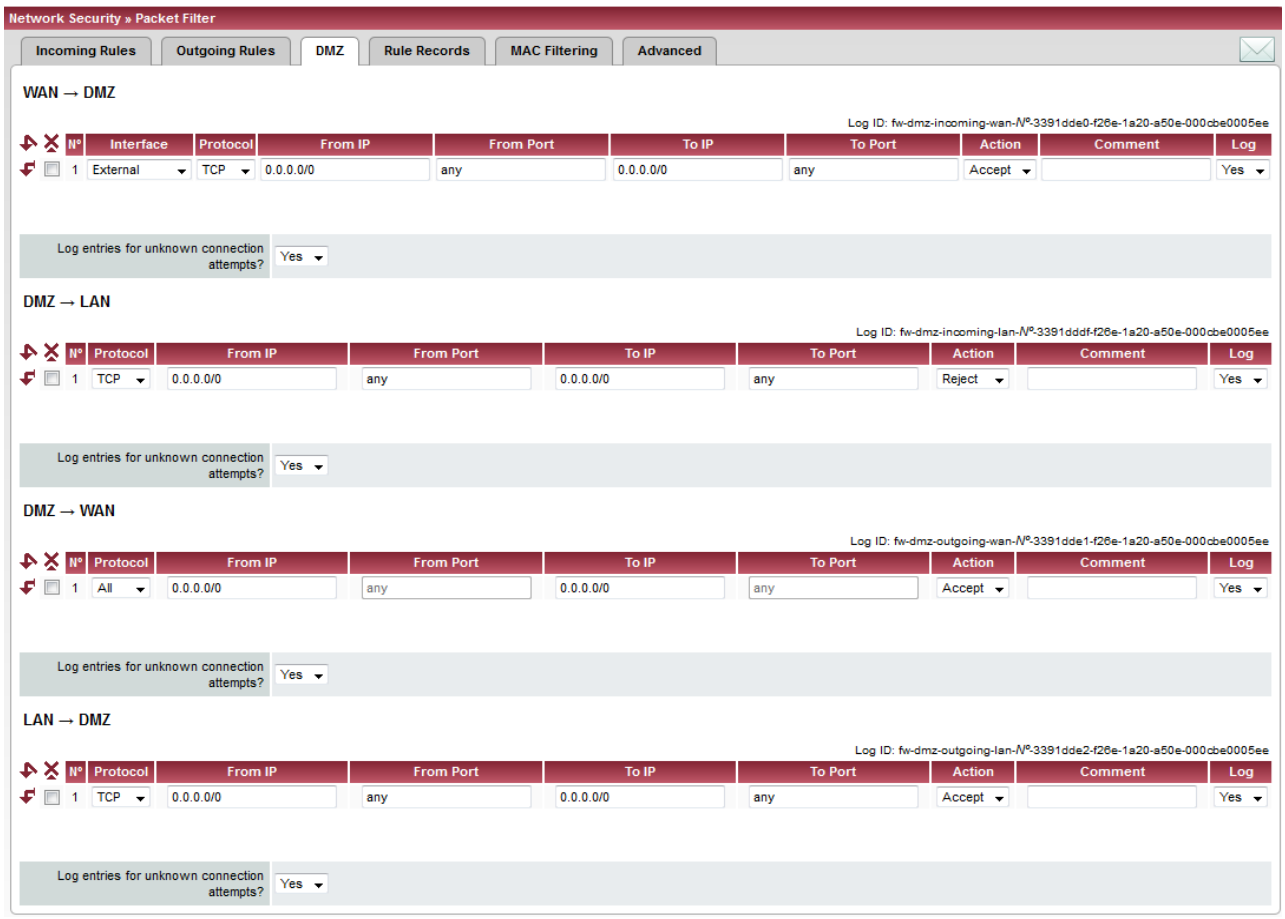
- **any** refers to any port.
- **startport:endport** (e.g., 110:120) refers to a port area.

Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).

Network Security >> Packet Filter >> Outgoing Rules [...]

Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. In Stealth mode, **Reject** has the same effect as **Drop**. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule sets**, if defined. When a name is specified for rule sets, the firewall rules saved under this name take effect (see Rule Records tab page).
Comment	Freely selectable comment for this rule.
Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default settings).
Log entries for unknown connection attempts	When set to **Yes**, all connection attempts that are not covered by the rules defined above are logged. (Default settings: **No**)

8.1.3 DMZ

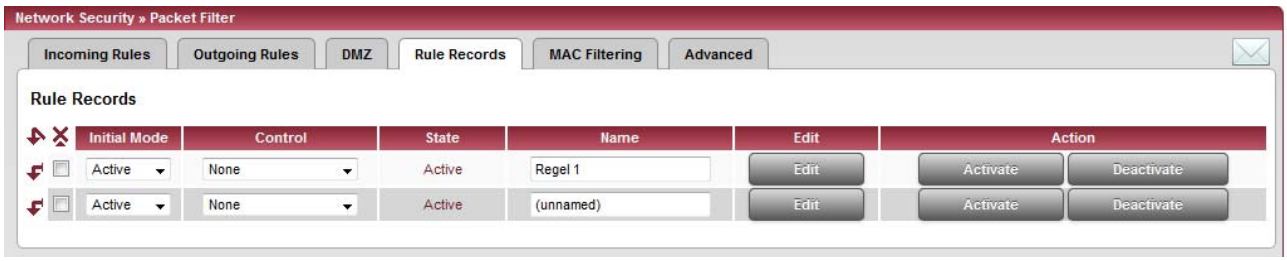

Network Security » Packet Filter
Incoming Rules
Outgoing Rules
DMZ
Rule Records
MAC Filtering
Advanced
WAN → DMZ
Log ID: fw-dmz-incoming-wan-N°-3391dde0-f26e-1a20-a50e-000cbe0005ee
N° Interface Protocol From IP From Port To IP To Port Action Comment Log
1 External TCP 0.0.0.0/0 any 0.0.0.0/0 any Accept Yes
Log entries for unknown connection attempts? Yes
DMZ → LAN
Log ID: fw-dmz-incoming-lan-N°-3391dddf-f26e-1a20-a50e-000cbe0005ee
N° Protocol From IP From Port To IP To Port Action Comment Log
1 TCP 0.0.0.0/0 any 0.0.0.0/0 any Reject Yes
Log entries for unknown connection attempts? Yes
DMZ → WAN
Log ID: fw-dmz-outgoing-wan-N°-3391dde1-f26e-1a20-a50e-000cbe0005ee
N° Protocol From IP From Port To IP To Port Action Comment Log
1 All 0.0.0.0/0 any 0.0.0.0/0 any Accept Yes
Log entries for unknown connection attempts? Yes
LAN → DMZ
Log ID: fw-dmz-outgoing-lan-N°-3391dde2-f26e-1a20-a50e-000cbe0005ee
N° Protocol From IP From Port To IP To Port Action Comment Log
1 TCP 0.0.0.0/0 any 0.0.0.0/0 any Accept Yes
Log entries for unknown connection attempts? Yes

Network Security >> Packet Filter >> DMZ

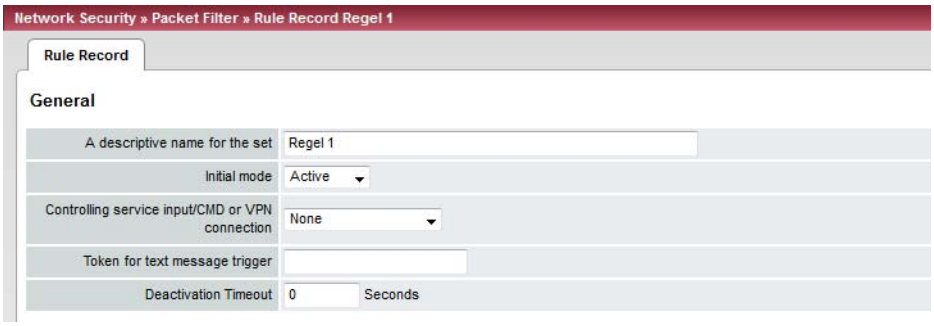
	Firewall rules for DMZ	
WAN → DMZ		Default: the data packets of all incoming connections are rejected.
DMZ → LAN		Default: the data packets of all incoming connections are rejected.
DMZ → WAN		Default: the data packets of all outgoing connections are allowed.
LAN → DMZ		Default: the data packets of all outgoing connections are allowed.
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols
	From IP/To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).

Network Security >> Packet Filter >> DMZ [...]		
	From Port/To Port	(Only evaluated for TCP and UDP protocols.) – **any** refers to any port. – **startport:endport** (e.g., 110:120) refers to a port area. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. In Stealth mode, **Reject** has the same effect as **Drop**. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule sets**, if defined. When a name is specified for rule sets, the firewall rules saved under this name take effect (see Rule Records tab page).
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default settings).
	Log entries for unknown connection attempts	When set to **Yes**, all connection attempts that are not covered by the rules defined above are logged. (Default settings: **No**)

8.1.4 Rule Records



Network Security >> Packet Filter >> Rule Records		
Rule Records	**Initial Mode**	**Active/Inactive/Disabled** Determines the output state of the firewall rule record following a reconfiguration or restart. The “Active/Inactive” setting is only applicable if a push button is connected. In case the firewall rule records are controlled via a switch or VPN connection, they have priority. If set to “Disabled”, the firewall rule record cannot be dynamically activated. The firewall rule record is retained but has no influence.
	Control	**Service input CMD 1-3, VPN connection** The firewall rule record can be switched via a push button/switch or a VPN connection. The push button/switch must be connected to one of the service contacts (CMD 1-3).
	State	Indicates the current state.
	Name	The firewall rule record can be freely named/renamed.
	Action	**Activate/Deactivate** If set to “Deactivate”, the rule record is deactivated.
Edit	The following tab page appears when you click on **Edit**:	



Network Security >> Packet Filter >> Rule Records [...]

General

A descriptive name for the set

The firewall rule record can be freely named/renamed.

Initial mode

Active/Inactive/Disabled

Determines the output state of the firewall rule record following a reconfiguration or restart.

The “Active/Inactive” setting is only applicable if a push button is connected. In case the firewall rule records are controlled via a switch or VPN connection, they have priority.

If set to “Disabled”, the firewall rule record cannot be dynamically activated. It is retained but has no influence.

Controlling service input/CMD or VPN connection

Service input CMD 1-3, VPN connection

The firewall rule record can be switched via a push button/switch or a VPN connection.

The push button/switch must be connected to one of the service contacts (CMD 1-3).

Token for text message trigger

Only available with the mGuard rs4000 3G

Incoming text messages can be used to activate or deactivate firewall rule records. The text message must contain the “fwrules/active” or “fwrules/inactive” command followed by the token.

Deactivation Timeout

Activated firewall rule records are deactivated after this time has elapsed.

0 means the setting is switched off.

Time in seconds (0 to 86400, 1 day)

Firewall rules

N°	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
1	TCP	0.0.0.0/0	any	0.0.0.0/0	any	Accept		No
2	TCP	0.0.0.0/0	any	0.0.0.0/0	any	Accept		No

Protocol

All means TCP, UDP, ICMP, GRE, and other IP protocols

From IP

0.0.0.0/0 means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).

From Port/To Port

(Only evaluated for TCP and UDP protocols.)

– **any** refers to any port.

– **startport:endport** (e.g., 110:120) refers to a port area.

Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).

Network Security >> Packet Filter >> Rule Records [...]

Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. In Stealth mode, **Reject** has the same effect as **Drop**. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule sets**, if defined. When a name is specified for rule sets, the firewall rules saved under this name take effect.
Comment	Freely selectable comment for this rule.
Log	For each firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default setting)

If a connection associated with a firewall rule record has been established and is continuously creating data traffic, deactivation of the firewall rule record might not interrupt this connection as expected.

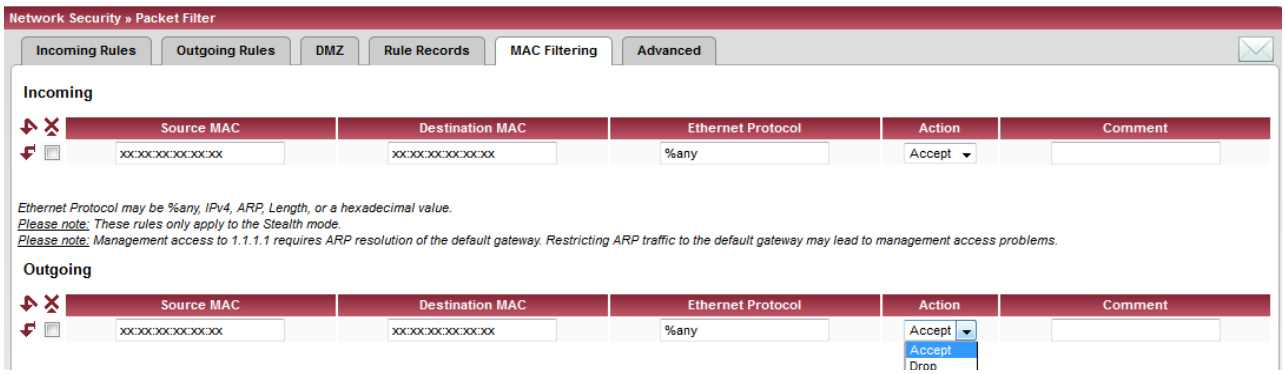
This happens because the (outgoing) response of a service on the LAN side creates an entry in the connection tracking table which enables a different (incoming) request from an external peer. This peer passes the firewall using the same parameters, however, it is not connected to the firewall rule record.

There are two ways to set up the mGuard so that it interrupts the associated connections when deactivating the firewall rule record.

– Activate the “Allow TCP connections upon SYN only” option under Network Security >> Packet Filter >> Advanced.
– In the firewall, block the outgoing connections that operate via the port that is the destination for the incoming connections.

  If, for example, the firewall rule record enables incoming data traffic on port 22, an outgoing rule can be set up that deactivates any data traffic coming from port 22.

8.1.5 MAC Filtering



The “Incoming” MAC filter is applied to frames that the mGuard receives at the WAN interface. The “Outgoing” MAC filter is applied to frames that the mGuard receives at the LAN interface. Data packets that are received or sent via a modem connection on models with a serial interface[1] are not picked up by the MAC filter because the Ethernet protocol is not used here.

In *Stealth* mode, in addition to the packet filter (Layer 3/4) that filters data traffic, e.g., according to ICMP messages or TCP/UDP connections, a MAC filter (Layer 2) can also be set. A MAC filter (Layer 2) filters according to MAC addresses and Ethernet protocols.

In contrast to the packet filter, the MAC filter is stateless. If rules are introduced, corresponding rules must also be created for the opposite direction.

If no rules are set, all ARP and IP packets are allowed to pass through.

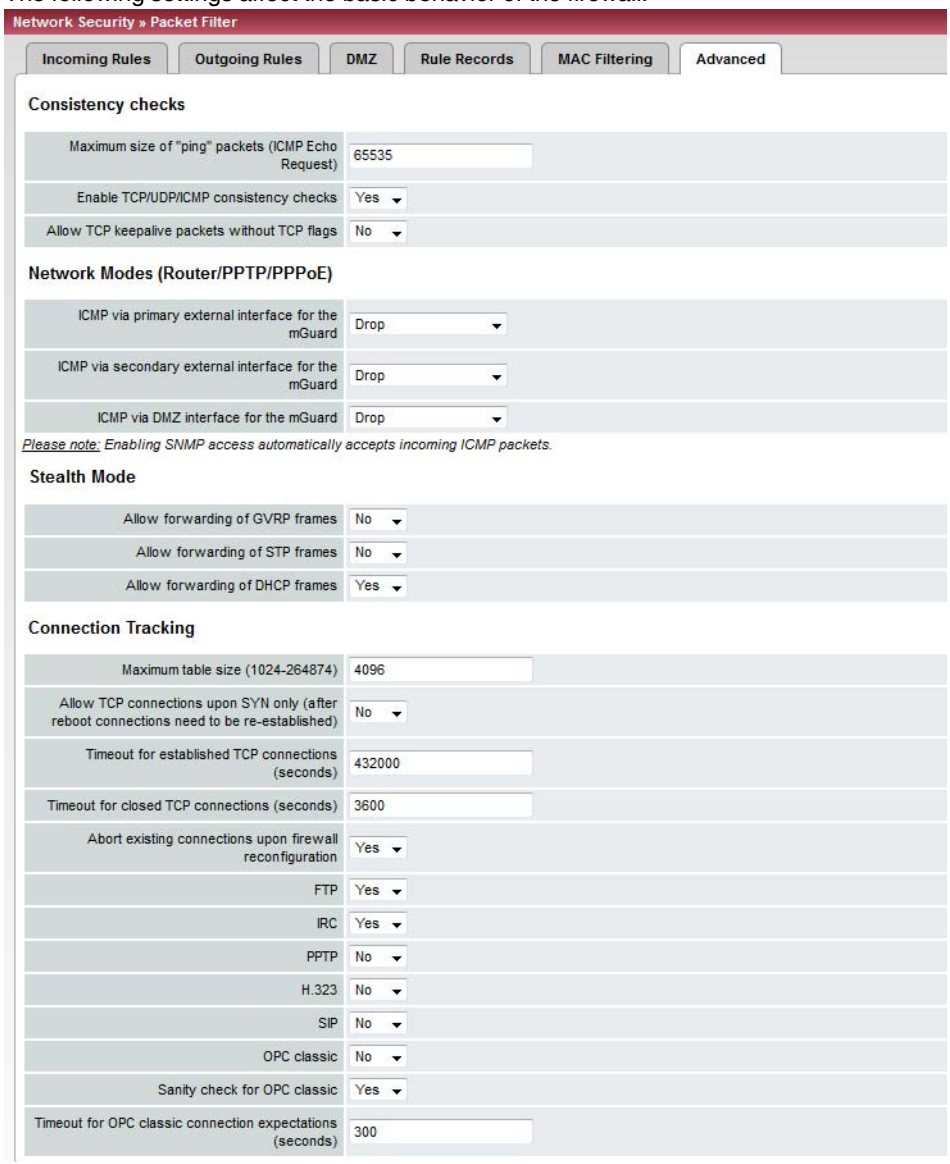
When setting MAC filter rules, please note the information displayed on the screen. The rules defined here have priority over packet filter rules. The MAC filter does not support logging.

Network Security >> Packet Filter >> MAC Filtering		
Incoming	**Source MAC**	Specification of the source MAC address: xx:xx:xx:xx:xx:xx stands for all MAC addresses.
	Destination MAC	Specification of the destination MAC address: xx:xx:xx:xx:xx:xx stands for all MAC addresses. ff:ff:ff:ff:ff:ff stands for the broadcast MAC address to which all ARP requests, for example, are sent.
	Ethernet Protocol	**%any** stands for all Ethernet protocols. Additional protocols can be specified in name or hexadecimal format, for example: – IPv4 or 0800 – ARP or 0806
	Action	**Accept** means that the data packets may pass through. **Drop** means that the data packets are not permitted to pass through (they are dropped).
	Comment	Freely selectable comment for this rule.
Outgoing	The explanation provided under “Incoming” also applies to “Outgoing”.	

[1] *mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs, mGuard blade, mGuard delta, EAGLE mGuard*

8.1.6 Advanced

The following settings affect the basic behavior of the firewall.



Network Security >> Packet Filter >> Advanced

Consistency checks This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.	**Maximum size of “ping” packets (ICMP Echo Request)**	Refers to the length of the entire packet including the header. The packet length is normally 64 bytes, but it can be larger. If oversized packets are to be blocked (to prevent bottlenecks), a maximum value can be specified. This value should be more than 64 bytes in order not to block normal ICMP echo requests.

Network Security >> Packet Filter >> Advanced [...]		
	Enable TCP/UDP/ICMP consistency checks	When set to **Yes**, the mGuard performs a range of tests to check for incorrect checksums, packet sizes, etc. and drops packets that fail these tests. This option is set to **Yes** by default.
	Allow TCP keepalive packets without TCP flags	TCP packets without flags set in their TCP header are normally rejected by firewalls. At least one type of Siemens controller with older firmware sends TCP keepalive packets without TCP flags set. These are therefore discarded as invalid by the mGuard. When set to **Yes**, forwarding of TCP packets where no TCP flags are set in the header is enabled. This only applies when TCP packets of this type are sent within an existing TCP connection established in the regular way. TCP packets without TCP flags do not result in a new entry in the connection table (see "Connection Tracking" on page 218). If the connection is already established when the mGuard is restarted, the corresponding packets are still rejected and connection problems can be observed as long as no packets with flags belonging to the connection are sent. These settings affect all the TCP packets without flags. The **Yes** option thus weakens the security functions provided by the mGuard.
Network Modes (Router/PPTP/PPPoE)	**ICMP via primary external interface for the mGuard** **ICMP via secondary external interface for the mGuard** **ICMP via DMZ for the mGuard**	This option can be used to control the behavior of the mGuard when ICMP messages are received from the external network via the primary/secondary external interface. Regardless of the setting specified here, incoming ICMP packets are always accepted if SNMP access is activated. **Drop**: all ICMP messages to the mGuard are dropped. **Allow ping requests**: only ping messages (ICMP type 8) to the mGuard are accepted. **Allow all ICMPs**: all ICMP message types to the mGuard are accepted.
Stealth Mode	**Allow forwarding of GVRP frames**	**Yes/No** The GARP VLAN Registration Protocol (GVRP) is used by GVRP-capable switches to exchange configuration information. If this option is set to **Yes**, GVRP packets are allowed to pass through the mGuard in *Stealth* mode.

Network Security >> Packet Filter >> Advanced [...]		
	Allow forwarding of STP frames	**Yes/No** The Spanning Tree Protocol (STP) (802.1d) is used by bridges and switches to detect and consider loops in the cabling. If this option is set to **Yes**, STP packets are allowed to pass through the mGuard in *Stealth* mode.
	Allow forwarding of DHCP frames	**Yes/No** When set to **Yes**, the client is allowed to obtain an IP address via DHCP - regardless of the firewall rules for outgoing data traffic. This option is set to **Yes** by default.
Connection Tracking	**Maximum table size**	This entry specifies an upper limit. This is set to a level that can never be reached during normal practical operation. However, it can be easily reached in the event of attacks, thus providing additional protection. If there are special requirements in your operating environment, this value can be increased. Connections established from the mGuard are also counted. This value must therefore not be set too low, as this will otherwise cause malfunctions.
	Allow TCP connections upon SYN only	**Yes/No, default: No** SYN is a special data packet used in TCP/IP connection establishment that marks the beginning of the connection establishment process. **No** (default): the mGuard also allows connections where the beginning has not been registered. This means that the mGuard can perform a restart when a connection is present without interrupting the connection. **Yes**: the mGuard must have registered the SYN packet of an existing connection. Otherwise, the connection is aborted. If the mGuard performs a restart while a connection is present, this connection is interrupted. Attacks on and the hijacking of existing connections are thus prevented.
	Timeout for established TCP connections (seconds)	If a TCP connection is not used during the time period specified here, the connection data is deleted. A connection translated by NAT (not 1:1 NAT) must then be reestablished. If **Yes** is set under “Allow TCP connections upon SYN only” , all expired connections must be reestablished. The default setting is 432000 seconds (5 days).

Network Security >> Packet Filter >> Advanced [...]		
	Timeout for closed TCP connections (seconds)	The timeout blocks a TCP port-to-port connection for an extended period after the connection is closed. This is necessary as packets belonging to the closed TCP connection may still arrive in a packet-based network after the connection is closed. Without time-controlled blocking, old packets could be assigned to a new connection accidentally. The default setting is 3600 seconds (1 hour).
	Abort existing connections upon firewall reconfiguration	**Yes/No, default: Yes** When set to **Yes**, the existing connections are reset if the following applies: – **Yes** is set under “Allow TCP connections upon SYN only” – The firewall rules have been adjusted – The value was changed from **No** to **Yes** (even without changing the firewall rules) After changing the firewall rules, the mGuard behaves in the same way as after a restart. However, this only applies to the forwarded connections. Existing TCP connections are interrupted, even if they are allowed according to the new firewall rules. Connections to the device are not affected, even if the firewall rules have been changed for the remote access. If set to **No**, the connections remain, even if the firewall rules changed would not allow or abort them.
	FTP	**Yes/No** If an outgoing connection is established to call data for the FTP protocol, two methods of data transmission can be used: With “active FTP”, the called server establishes an additional counter-connection to the caller in order to transmit data over this connection. With “passive FTP”, the client establishes this additional connection to the server for data transmission. FTP must be set to **Yes** (default) so that additional connections can pass through the firewall.
	IRC	**Yes/No** Similar to FTP: for IRC chat over the Internet to work properly, incoming connections must be allowed following active connection establishment. IRC must be set to **Yes** (default) in order for these connections to pass through the firewall.

Network Security >> Packet Filter >> Advanced [...]		
	PPTP	**Yes/No, default: No** Must be set to **Yes** if VPN connections are to be established using PPTP from local computers to external computers without the assistance of the mGuard. Must be set to **Yes** if GRE packets are to be forwarded from the internal area to the external area.
	H.323	**Yes/No, default: No** Protocol used to establish communication sessions between two or more devices. Used for audio-visual transmission. This protocol is older than SIP.
	SIP	**Yes/No, default: No** SIP (Session Initiation Protocol) is used to establish communication sessions between two or more devices. Often used in IP telephony. When set to **Yes**, it is possible for the mGuard to track the SIP and add any necessary firewall rules dynamically if further PCP channels are established to the same session. When NAT is also activated, one or more locally connected computers can communicate with external computers by SIP via the mGuard.
	OPC classic	This function can only be activated when a suitable license key (OPC Inspector) is installed. With OPC Classic, communication always starts via port 135. The client and server then negotiate one or more additional connections on new ports. To enable these connections, all ports of an interconnected firewall needed to be open until now. If **OPC classic** is activated, it is enough to only enable port 135 for a client/server pair using the firewall rules. The mGuard inspects the user data of the packets (deep packet inspection). It checks in the user data sent via this port whether a new connection has been negotiated, and opens the negotiated port. To do so, communication between the client and the server on port 135 must be enabled in both directions. If **OPC classic** is activated, NAT procedures can be used. If masquerading is to be used, port forwarding of port 135 to the OPC server/client must be activated on the LAN interface of the mGuard.
	Sanity check for OPC classic	If the **Sanity check for OPC classic** is activated, only OPC packets must be transmitted via OPC Classic port 135 and the newly negotiated ports.

Network Security >> Packet Filter >> Advanced [...]		
	Timeout for OPC classic connection expectations	Configures the timeout during which OPC traffic is expected. An existing OPC connection may negotiate another connection on a new port. If the “Sanity check for OPC classic” is activated, these connections must only be OPC connections. The mGuard opens a port for the new connection by adding a temporary firewall rule. After the time set here has elapsed, the firewall rule is removed again. After that, new connections can no longer be established via this port. Existing connections are retained.

8.1.7 Firewall for the mGuard rs2000 (3G)

The mGuard rs2000 (3G) has a simple “2-click firewall”. This either permits or rejects all incoming and outgoing connections. No advanced settings are provided. Furthermore, access via this firewall is not logged (see *Logging >> Browse local logs*).

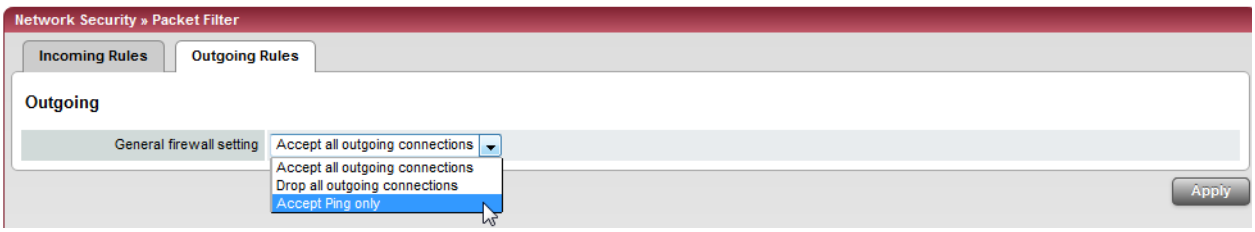
The following firewall functionality is available when using the **mGuard rs2000** or **mGuard rs2000 3G**:

Incoming Rules

– Accept all incoming connections
– Drop all incoming connections
– Accept Ping only
  This setting allows all ping packets to pass. The integrated protection against brute force attacks is not effective in this case.

Outgoing Rules

– Accept all outgoing connections
– Drop all outgoing connections
– Accept Ping only
  This setting allows all ping packets to pass. The integrated protection against brute force attacks is not effective in this case.

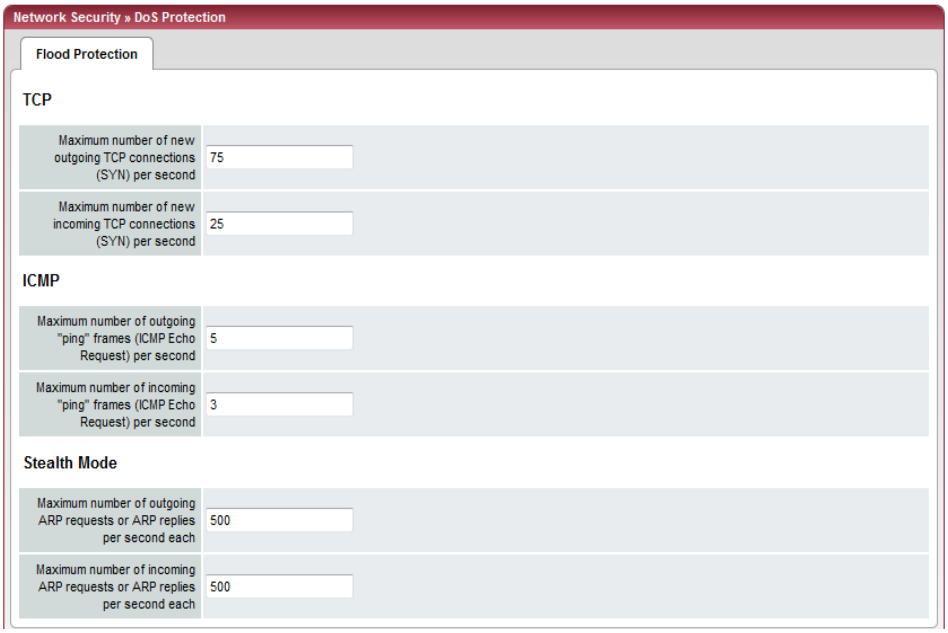


These variables are also available on other devices. However, other devices also have advanced settings (see “Incoming rules” on page 206 and “Outgoing rules” on page 208).

8.2 Network Security >> DoS Protection

8.2.1 Flood Protection

This menu is **not** available on the **mGuard rs2000 (3G)**.


Network Security » DoS Protection
Flood Protection
TCP
Maximum number of new outgoing TCP connections (SYN) per second
75
Maximum number of new incoming TCP connections (SYN) per second
25
ICMP
Maximum number of outgoing "ping" frames (ICMP Echo Request) per second
5
Maximum number of incoming "ping" frames (ICMP Echo Request) per second
3
Stealth Mode
Maximum number of outgoing ARP requests or ARP replies per second each
500
Maximum number of incoming ARP requests or ARP replies per second each
500

Network Security >> DoS Protection >> Flood Protection		
TCP	**Maximum number of new incoming/outgoing TCP connections (SYN) per second**	Outgoing: default setting: 75 Incoming: default setting: 25 Maximum values for the number of incoming and outgoing TCP connections allowed per second. These values are set to a level that can never be reached during normal practical operation. However, they can be easily reached in the event of attacks, thus providing additional protection. If there are special requirements in your operating environment, these values can be increased.

Network Security >> DoS Protection >> Flood Protection [...]		
ICMP	**Maximum number of incoming/outgoing “ping” frames (ICMP Echo Request) per second**	Outgoing: default setting: 5 Incoming: default setting: 3 Maximum values for the number of incoming and outgoing “ping” packets allowed per second. These values are set to a level that can never be reached during normal practical operation. However, they can be easily reached in the event of attacks, thus providing additional protection. If there are special requirements in your operating environment, these values can be increased. Value **0** means that no “ping” packets are allowed through or in.
Stealth Mode	**Maximum number of incoming/outgoing ARP requests or ARP replies per second each**	Default setting: 500 Maximum values for the number of incoming and outgoing ARP requests or replies allowed per second. These values are set to a level that can never be reached during normal practical operation. However, they can be easily reached in the event of attacks, thus providing additional protection. If there are special requirements in your operating environment, these values can be increased.

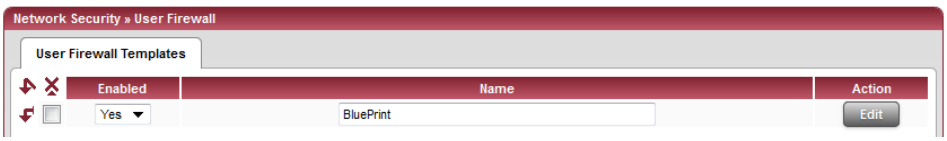
8.3 Network Security >> User Firewall

This menu is **not** available on the **mGuard rs2000 (3G)**.

The user firewall is used exclusively by firewall users, i.e., users that are registered as firewall users (see “Authentication >> Firewall Users” on page 185).

Each firewall user can be assigned a set of firewall rules, also referred to as a template.

8.3.1 User Firewall Templates



All defined user firewall templates are listed here. A template can consist of several firewall rules. A template can be assigned to several users.

Defining a new template:

- In the template table, click on **Edit** to the right of the “(unnamed)” entry under “Name”.
- If the “(unnamed)” entry cannot be seen, open another row in the table.

Editing a set of rules:

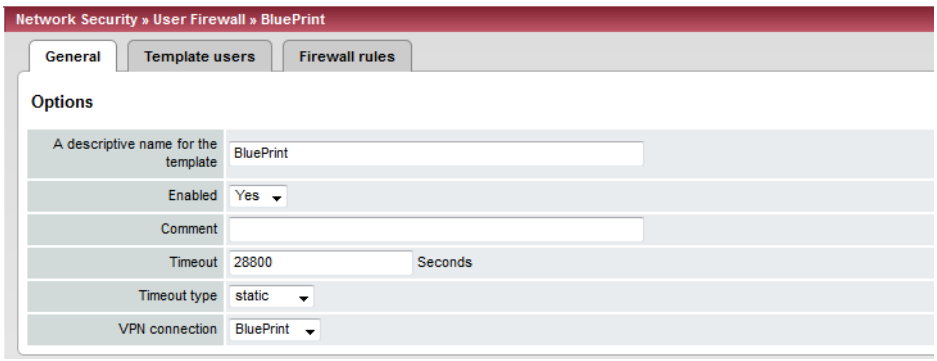
- Click on **Edit** to the right of the relevant entry.

Network Security >> User Firewall >> User Firewall Templates	
Enabled	Activates/deactivates the relevant template.
Name	Name of the template. The name is specified when the template is created.

Network Security >> User Firewall >> User Firewall Templates [...]

General

The following tab page appears when you click on **Edit**:



Options

A descriptive name for the template

The user firewall template can be freely named and renamed.

Enabled

Yes/No

When set to **Yes**, the user firewall template becomes active as soon as firewall users log into the mGuard who are listed on the *Template users* tab page (see below) and who have been assigned this template. It does not matter from which computer and under what IP address the user logs in. The assignment of the firewall rules to a user is based on the authentication data that the user enters during login (user name, password).

Comment

Optional explanatory text.

Timeout

Default: 28800.

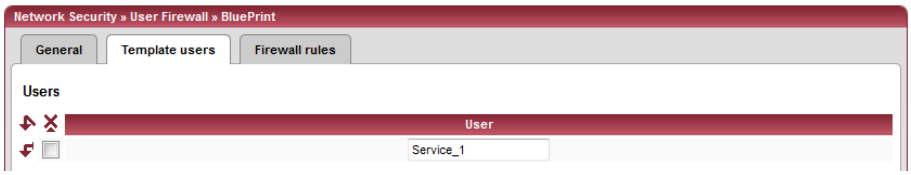
Specifies the time in seconds at which point the firewall rules are deactivated. If the user session lasts longer than the timeout time specified here, the user has to log in again.

Network Security >> User Firewall >> User Firewall Templates [...]

Timeout type	static/dynamic With a *static* timeout, users are logged out automatically as soon as the set timeout time has elapsed. With *dynamic* timeout, users are logged out automatically after all the connections have been closed by the user or have expired on the mGuard, and the set timeout time has elapsed. An mGuard connection is considered to have expired if no more data is sent for this connection over the following periods.
Connection expiration period after non-usage	
– TCP	5 days (this value can be set, see “Timeout for established TCP connections (seconds)” on page 218.) 120 seconds are added after closing the connection. (This also applies to connections closed by the user.)
– UDP	30 seconds after data traffic in one direction; 180 seconds after data traffic in both directions
– ICMP	30 seconds
– Others	10 minutes
VPN connection	Specifies the VPN connection for which this user firewall rule is valid. This requires an existing remote access through the VPN tunnel to the web interface.

Network Security >> User Firewall >> User Firewall Templates >> Edit > ...

Template users



Specify the names of the users here. The names must correspond to those that have been defined under the Authentication >> Firewall Users menu (see Page 185).

Firewall rules

Source IP

IP address from which connections are allowed to be established. If this should be the address from which the user logged into the mGuard, the wildcard "%authorized_ip" should be used.

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

Protocol

All means TCP, UDP, ICMP, GRE, and other IP protocols

From Port/To Port

(Only evaluated for TCP and UDP protocols.)

- **any** refers to any port.
- **startport:endport** (e.g., 110:120) > port area.

Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).

To IP

0.0.0.0/0 means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 24).

Comment

Freely selectable comment for this rule.

Log

For each firewall rule, you can specify whether the use of the rule:

- Should be logged – set *Log* to **Yes**
- Should not be logged – set *Log* to **No** (default setting)

9 CIFS Integrity Monitoring menu

CIFS integrity monitoring is **not** available on the **mGuard rs2000 (3G)**.

It must **not** be used on the **mGuard blade controller**.

In Stealth network mode, CIFS integrity checking is not possible without a management IP address and the CIFS server for the anti-virus scan is not supported.

There are two options for checking network drives for viruses using CIFS integrity monitoring.

– CIFS Integrity Checking
– CIFS Antivirus Scan Connector

CIFS Integrity Checking

When **CIFS integrity checking** is performed, the Windows network drives are checked to determine whether certain files (e.g., *.exe, *.dll) have been changed. Changes to these files indicate a possible virus or unauthorized intervention.

CIFS Antivirus Scan Connector

The **CIFS Antivirus Scan Connector** enables the mGuard to perform a virus scan on drives that are otherwise not externally accessible (e.g., production cells). The mGuard mirrors a drive externally in order to perform the virus scan. Additional anti-virus software is required for this procedure. Set the necessary read access for your anti-virus software.

Setting options for CIFS integrity checking

– Which network drives are known to the mGuard (see “CIFS Integrity Monitoring >> Importable Shares” on page 230).
– What type of access is permitted (see “CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings” on page 233).
– At what intervals the drives should be checked (see “CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Checked Share” on page 235).
– Which file types should be checked (see “CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns” on page 240).
– Warning method when a change is detected (e.g., via e-mail, see “CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings” on page 233 or via SNMP, see “CIFS integrity traps” on page 87).

Setting options for the CIFS Antivirus Scan Connector

– Which network drives are known to the mGuard (see “CIFS Integrity Monitoring >> Importable Shares” on page 230).
– What type of access is permitted (read or read/write access, see “CIFS Integrity Monitoring >> CIFS AV Scan Connector” on page 242).

9.1 CIFS Integrity Monitoring >> Importable Shares

Requirements:

The network drives that the mGuard should check regularly can be specified here.

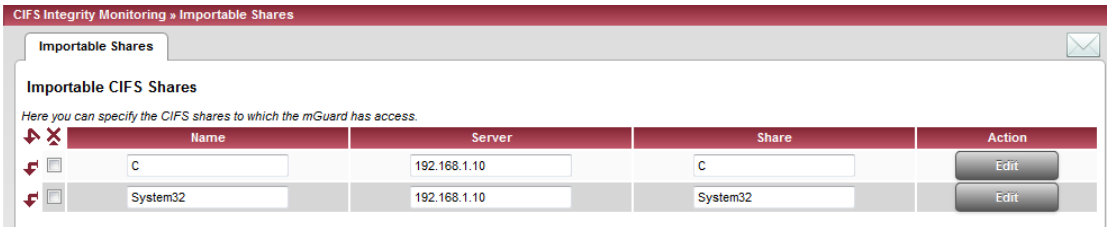
In order for the network drives to be checked, you must also refer to these network drives in one of the two methods (CIFS integrity checking or CIFS Antivirus Scan Connector).

The references to the network drives can be set as follows:

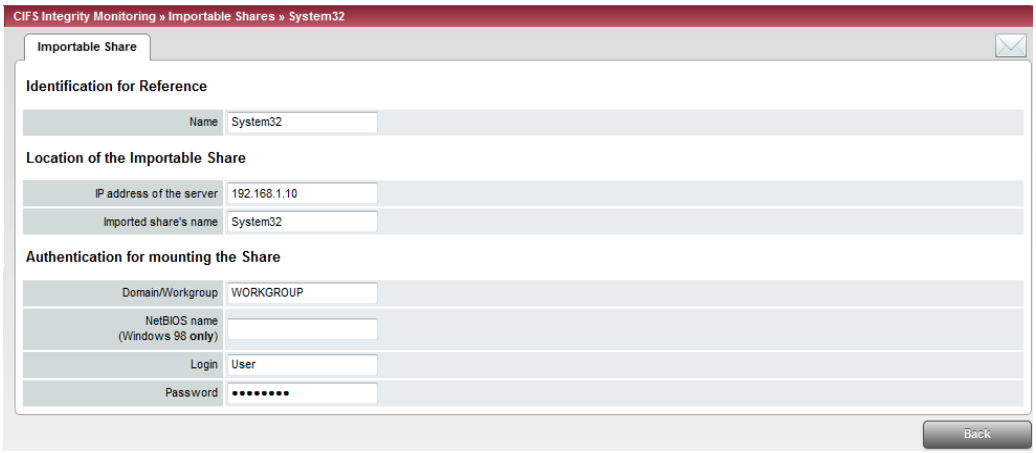
– For CIFS integrity checking, see “Checked CIFS Share” on page 234.

– For CIFS Antivirus Scan Connector, see “CIFS Antivirus Scan Connector” on page 242.

9.1.1 Importable Shares



CIFS Integrity Monitoring >> Importable Shares		
Importable CIFS Shares	**Name**	Name of the network drive to be checked. (Internal name used in the configuration).
	Server	IP address of the authorizing server.
	CIFS Share	Name of the network drive made available by the authorizing server.
		Click on **Edit** to make the settings.



CIFS Integrity Monitoring >> Importable Shares >> Edit		
Identification for Reference	**Name**	Name of the network drive to be checked (Internal name used in the configuration).
Location of the importable share	**IP address of the server**	IP address of the server whose network drive is to be checked.
	Imported share's name	Directory on the above authorized server that is to be checked.
Authentication for mounting the Share	**Domain/workgroup**	Name of the workgroup to which the network drive belongs.
	NetBIOS name (Windows 95/98 only)	NetBIOS name for Windows 95/98 computers
	Login	Login for the server.
	Password	Password for login.

9.2 CIFS Integrity Monitoring >> CIFS Integrity Checking

When **CIFS integrity checking** is performed, the Windows network drives are checked to determine whether certain files (e.g., *.exe, *.dll) have been changed. Changes to these files indicate a possible virus or unauthorized intervention.

Integrity database

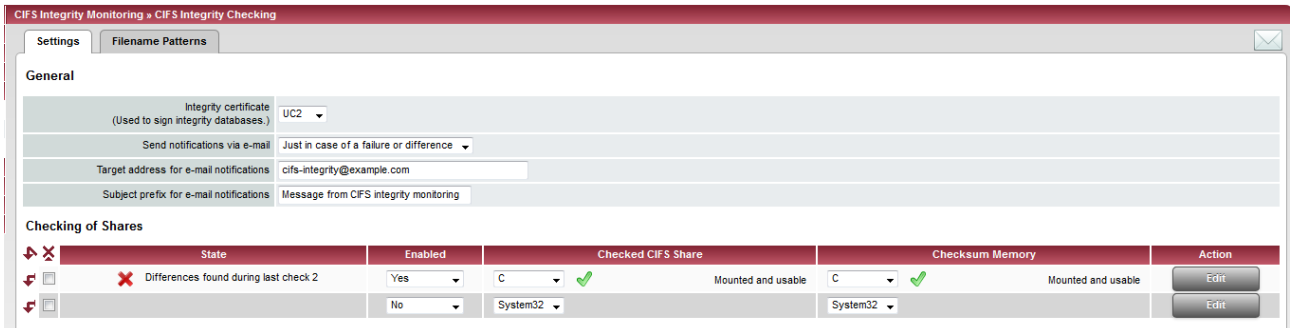
If a network drive that is to be checked is reconfigured, an integrity database must be created.

This integrity database is used as the basis for comparison when checking the network drive regularly. The checksums of all files to be monitored are recorded here. The integrity database is protected against manipulation.

The database is either created explicitly due to a specific reason (see *CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management, Possible Actions*) or on the first regular check of the drive.

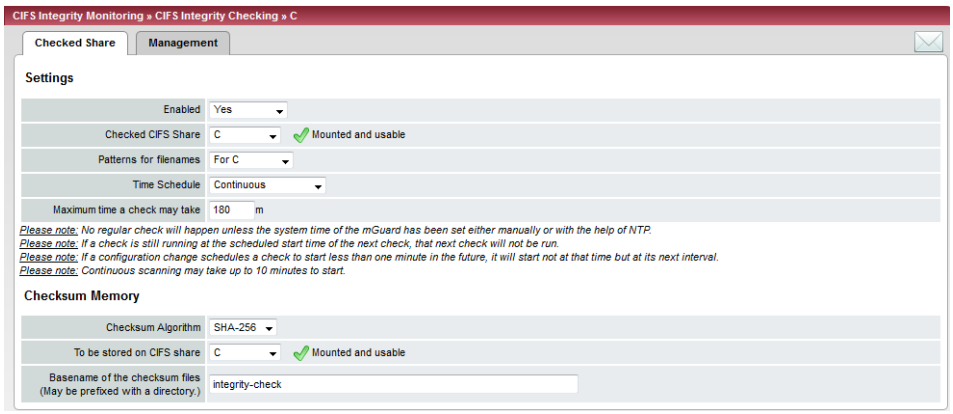
The integrity database must be created again following intentional manipulation of the relevant files of the network drive. Unauthorized manipulation of the relevant files cannot be detected if there is no (valid) integrity database.

9.2.1 Settings



CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings		
General	**Integrity certificate (used to sign integrity databases)**	Used for signing and checking the integrity database so that it cannot be replaced or manipulated by an intruder without being detected. For information about certificates, please refer to “Machine Certificates” on page 197.
	Send notifications via e-mail	**After every check**: an e-mail is sent to the address specified below after every check. **No**: an e-mail is not sent to the address specified below. **Only with faults and deviations**: an e-mail is sent to the address specified below if a deviation is detected during CIFS integrity checking or if the check could not be carried out due to an access error.
	E-mail address for notifications	An e-mail is sent to this address either after every check or only if a deviation is detected during CIFS integrity checking or if the check could not be carried out due to an access error.
	Start of the subject for e-mail notifications	Text entered in the subject field of the e-mail.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings [...]		
Checking of Shares	**State**	– No check is currently being performed – The share check has been suspended – A drive check is currently in progress – An integrity database is currently being created – The share has not yet been checked. Probably no integrity database exists. – Last check finished successfully – The process failed due to an unforeseen condition, please consult the logs – Last check was aborted due to timeout. – The integrity database is missing or incomplete. – The signature of the integrity database is invalid. – The integrity database was created with a different hash algorithm. – The integrity database is the wrong version. – The share which is to be checked is not available. – The share which is to be used as checksum memory is not available. – A file could not be read due to an I/O failure. Please consult the report. – The directory tree could not be traversed due to an I/O failure. Please consult the report. – The signature has not yet been checked – The signature is valid
	Enabled	**No**: a check is not triggered for this network drive. The mGuard has not connected this drive. The status cannot be viewed. **Yes**: a check is triggered regularly for this network drive. **Suspended**: the check has been suspended until further notice. The status can be viewed.
	Checked CIFS Share	Name of the network drive to be checked (specified under *CIFS Integrity Monitoring >> Importable Shares >> Edit*).
	Checksum Memory	In order to perform the check, the mGuard must be provided with a network drive for storing the files. The checksum memory can be accessed via the external network interface.
Action	Click on **Edit** to make further settings for checking network drives.	


CIFS Integrity Monitoring » CIFS Integrity Checking » C
Checked Share
Management
Settings
Enabled
Yes
Checked CIFS Share
C
Mounted and usable
Patterns for filenames
For C
Time Schedule
Continuous
Maximum time a check may take
180
m
Please note: No regular check will happen unless the system time of the mGuard has been set either manually or with the help of NTP.
Please note: If a check is still running at the scheduled start time of the next check, that next check will not be run.
Please note: If a configuration change schedules a check to start less than one minute in the future, it will start not at that time but at its next interval.
Please note: Continuous scanning may take up to 10 minutes to start.
Checksum Memory
Checksum Algorithm
SHA-256
To be stored on CIFS share
C
Mounted and usable
Basename of the checksum files (May be prefixed with a directory.)
integrity-check

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Checked Share

Settings

Enabled

No: a check is not triggered for this network drive. The mGuard has not connected this drive. The status cannot be viewed.

Yes: a check is triggered regularly for this network drive.

Suspended: the check has been suspended until further notice. The status can be viewed.

Checked CIFS Share

Name of the network drive to be checked (specified under *CIFS Integrity Monitoring >> Importable Shares >> Edit*).

Patterns for filenames

Specific file types are checked (e.g., only executable files such as *.exe and *.dll).

The rules can be defined under *CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns*.

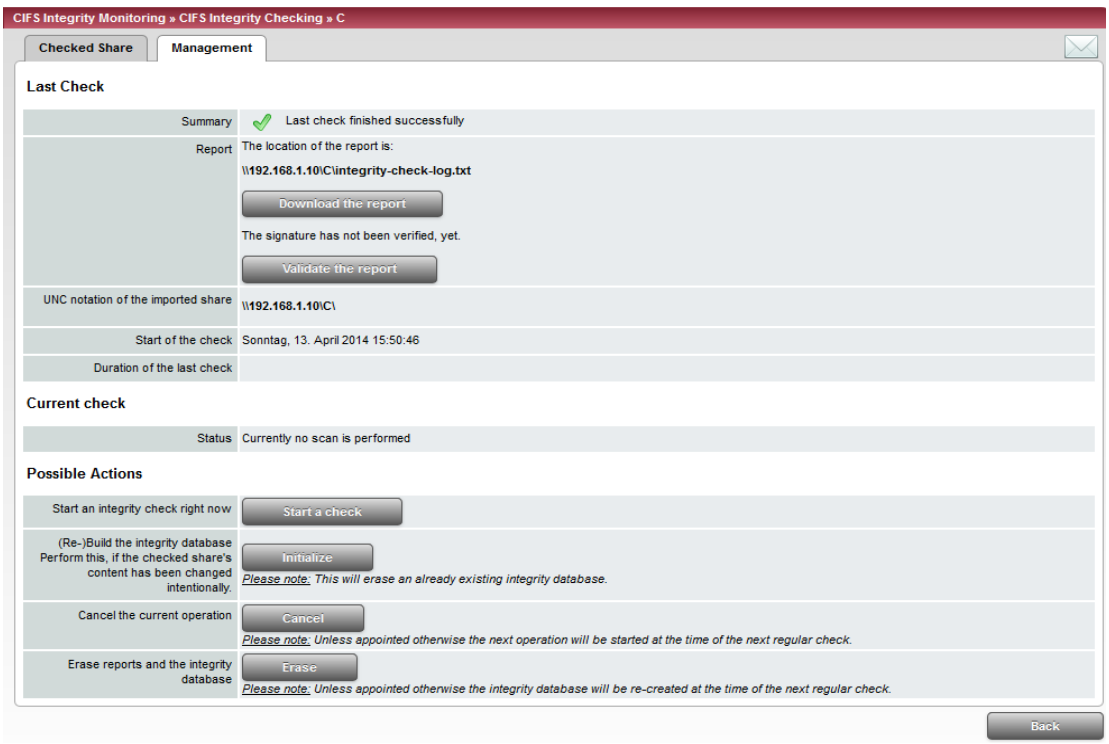
Do not check files that are changed in normal operation, as this could trigger false alarms.

Do not check files that are simultaneously opened **exclusively** by other programs, as this can lead to access conflicts.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Checked Share [...]		
	Time Schedule	Every Sunday, Every Monday, Every Tuesday, ... , Everyday, Several times a day, Continuous You can start the check every day, several times per day or on a specific weekday. The mGuard system time must be set for the time schedule to work properly. Integrity checks are not performed if the system time is not synchronized. This can be carried out manually or via NTP (see “Time and Date” on page 35). A check is only started if the mGuard is operating at the set time. If it is not operating at the time, a check is not performed later when the mGuard is started up again. The check can also be started manually (*CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management*, *Possible Actions*).
	Starting at	Time at which the check starts (hour, minute). If “Several times a day” is selected, every 1 h, 2 h, 3 h, 4 h, 6 h, 8 h, 12 h
	Maximum time a check may take	Maximum duration of the check sequence in minutes. You can thus ensure that the check is completed in good time (e.g., before a shift starts).
Checksum Memory	**Checksum Algorithm**	**SHA-1** **MD5** **SHA-256** Checksum algorithms such as MD5, SHA-1 or SHA-256 are used to check whether a file has been changed. SHA-256 is more secure than SHA-1, but it takes longer to process.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Checked Share [...]

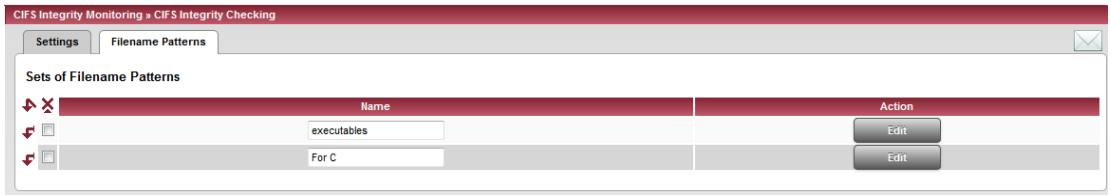
To be stored on CIFS share	In order to perform the check, the mGuard must be provided with a network drive for storing the files. The checksum memory can be accessed via the external network interface. The same network drive can be used as the checksum memory for several different drives to be checked. The base name of the checksum files must then be clearly selected in this case. The mGuard recognizes which version the checksum files on the network drive must have. For example, if it is necessary to restore the contents of the network drive from a backup following a malfunction, old checksum files are provided in this case and the mGuard would detect the deviations. In this case, the integrity database must be recreated (see *CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management*, *Possible Actions*).
Basename of the checksum files (May be prefixed with a directory.)	The checksum files are stored on the network drive specified above. They can also be stored in a separate directory. The directory name must not start with a backslash (\). Example: Checksumdirectory\integrity-checksum “Checksumdirectory” is the directory and contains the files beginning with “integrity-checksum”.


CIFS Integrity Monitoring » CIFS Integrity Checking » C
Checked Share
Management
Last Check
Summary
Last check finished successfully
Report
The location of the report is:
\\192.168.1.10\C\integrity-check-log.txt
Download the report
The signature has not been verified, yet.
Validate the report
UNC notation of the imported share
\\192.168.1.10\C\
Start of the check
Sonntag, 13. April 2014 15:50:46
Duration of the last check
Current check
Status
Currently no scan is performed
Possible Actions
Start an integrity check right now
Start a check
(Re-)Build the integrity database Perform this, if the checked share's content has been changed intentionally.
Initialize
Please note: This will erase an already existing integrity database.
Cancel the current operation
Cancel
Please note: Unless appointed otherwise the next operation will be started at the time of the next regular check.
Erase reports and the integrity database
Erase
Please note: Unless appointed otherwise the integrity database will be re-created at the time of the next regular check.
Back

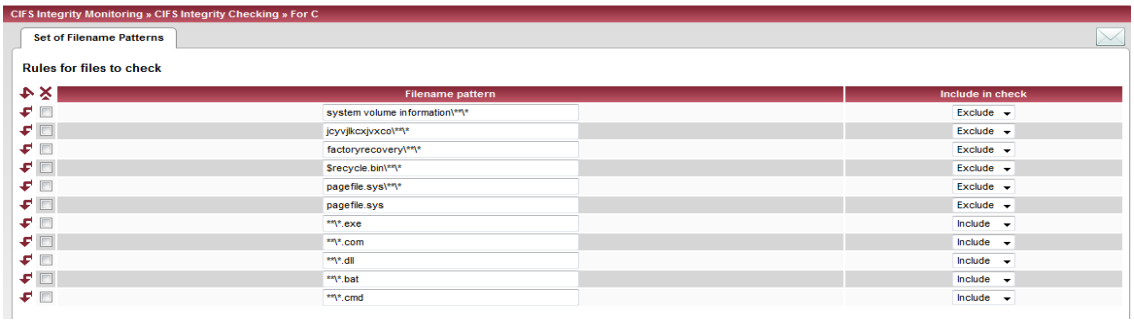
CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management		
Last check	**Summary**	**Last check was OK**: no deviations found. **Deviations detected during the last check: x** The exact deviations are listed in the check report.
	Report	The check report is displayed here. It can be downloaded by clicking on "**Download the report"**. Click on "**Validate the report"** to check whether the report is unchanged from the definition in the MGUARD (according to the signature and certificate).
	UNC notation of the imported share	\\Servername\networkdrive\
	Start of the last check	Weekday, month, day, HH:MM:SS (UTC). The local time may differ from this time. **Example**: the standard time in Germany is Central European Time (CET), which is UTC plus one hour. Central European Summer Time applies in summer, which is UTC plus two hours.
	Duration of the last check	Duration of the check in hours and minutes. (Only displayed if a check has been carried out.)
	Start of the current check	(Only displayed if a check has been carried out.)
	Progress of the current check	(Only displayed if a check is currently active.)
Current check	**Status**	Status of the integrity check
	Starts at	Start time
	Progress	Progress as a percentage and the number of checked files
	Number of detected deviations	Number of differences detected
	Estimated completion time	Estimated completion time for the check
Possible Actions	**Start an integrity check right now**	Click on **Start a check** to start the integrity check. Only displayed if a check is not currently active.
	(Re-)Build the integrity database	The mGuard creates a database with checksums in order to check whether files have been changed. A change to executable files indicates a virus. However, if these files have been changed intentionally, a new database must be created by clicking on **Initialize** in order to prevent false alarms. The creation of an integrity database is also recommended if network drives have been newly set up. Otherwise, an integrity database is set up during the first scheduled check instead of a check being performed.
	Interrupt the current process	Click on **Cancel** to stop the integrity check.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management [...]		
	Erase reports and the integrity database	Click on **Erase** to delete all existing reports/databases. A new integrity database must be created for any further integrity checks. This can be initiated by clicking on **Initialize.** Otherwise, a new integrity database is created automatically upon the next scheduled check. This procedure cannot be seen.

9.2.2 Filename Patterns



CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns		
Sets of Filename Patterns	**Name**	Freely definable name for a set of rules for the files to be checked. This name must be selected under **CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit** in order for the sample to be activated. Click on **Edit** to define a set of rules for the files to be checked and save this under the defined name.



CIFS Integrity Monitoring >> CIFS Integrity Checking >> Set of Filename Patterns >> Edit		
Rules for files to check	**Filename pattern**	The following rules apply: ****.exe* means that the files located in a specific directory and with file extension **.exe* are checked (or excluded). Only one wildcard (*) is permitted per directory or file name. Wildcards represent characters, e.g., *win**.exe* returns files with the extension **.exe* that are located in a directory that begins with *win...* **** at the start means that any directory is searched, even those at the top level (if this is empty). This cannot be combined with other characters (e.g., *c*** is not permitted). Example: *Name***.exe* refers to all files with the extension **.exe* that are located in the "*Name*" directory and any subdirectories.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Set of Filename Patterns >> Edit [...]

Missing files trigger an alarm. Missing files are files that were present during initialization.

An alarm is also triggered if additional files are present.

Include in check

Include: the files are included in the check.

(Each file name is compared with the samples one after the other. The first hit determines whether the file is to be included in the integrity check. The file is not included if no hits are found.)

Exclude: the files are excluded from the check.

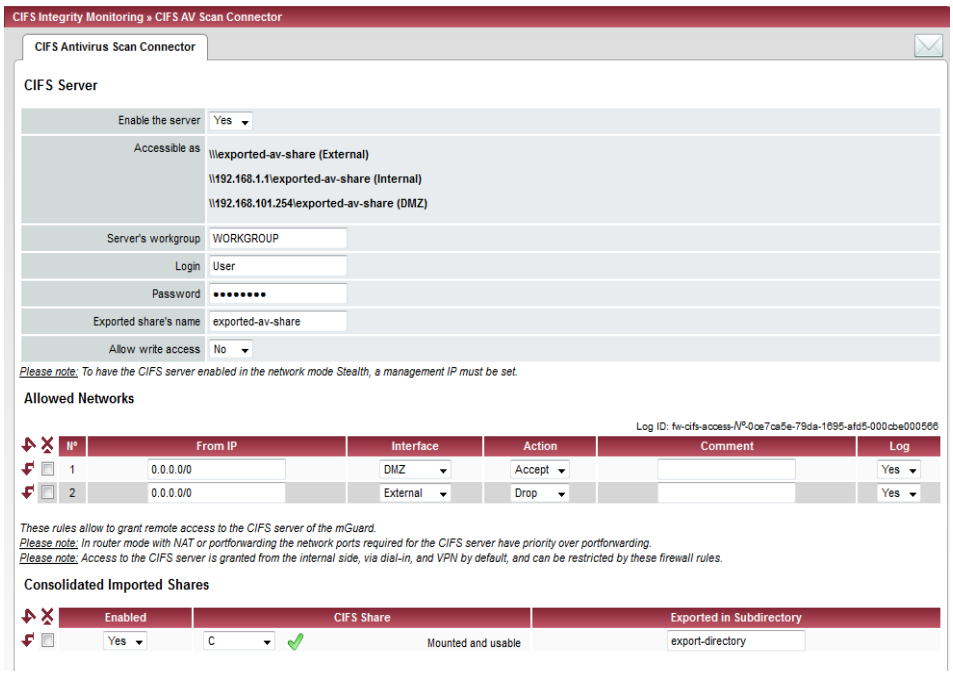
9.3 CIFS Integrity Monitoring >> CIFS AV Scan Connector

In Stealth network mode without management IP address, the CIFS server for the anti-virus scan is not supported.

CIFS Antivirus Scan Connector

The **CIFS Antivirus Scan Connector** enables the mGuard to perform a virus scan on drives that are otherwise not externally accessible (e.g., production cells). The mGuard mirrors a drive externally in order to perform the virus scan. Additional anti-virus software is required for this procedure. Set the necessary read access for your anti-virus software.

9.3.1 CIFS Antivirus Scan Connector



CIFS Integrity Monitoring >> CIFS AV Scan Connector		
CIFS Server	**Enable the server**	**No**: CIFS server is not available **Yes**: CIFS server is available

CIFS Integrity Monitoring >> CIFS AV Scan Connector[...]		
	Accessible as	**External/Internal/DMZ** Displays the virtual network drive provided by the mGuard for the “CIFS Antivirus Scan Connector” function. This path is displayed with UNC notation. By means of copy and paste, it can be directly used on the PC which is to use the virtual network drive (see“Accessing the virtual network (CIFS Antivirus Scan Connector)” on page 245). Three UNC addresses (for the internal and external interface and DMZ) are displayed in “Router” network mode, while one UNC address is displayed in “Stealth” network mode. Access to the virtual network drive can be prevented as a result of the settings in the “Allowed Networks” section. Enter a rule here accordingly, especially if access via the external interface is required. Depending on the mGuard configuration, further access options can be established over other IP addresses, such as access via VPN channels or via incoming calls (for dial-in, see “Dial-in” on page 136).
	Server's workgroup	Name of the CIFS server workgroup.
	Login	Login for the server.
	Password	Password for login.
	Exported share's name	Name for the computers that are to use the CIFS server to access the combined drives. (The drives are connected under this name).
	Allow write access	**No**: read-only access **Yes**: read and write access
Allowed Networks	These rules allow external access to the CIFS server of the mGuard. In Router mode with NAT or port forwarding, the port numbers for the CIFS server have priority over the rules for port forwarding (Port forwarding is set under “Network >> NAT”). Access to the CIFS server is approved internally via incoming calls (dial-in) and VPN as standard, and can be restricted or expanded via the firewall rules. A different default setting can also be defined using these rules.	
	From IP	Enter the address of the computer/network from which remote access is permitted or forbidden in this field. IP address **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).

CIFS Integrity Monitoring >> CIFS AV Scan Connector[...]		
	Interface	**External/Internal/External 2/VPN/Dial-in[1]/DMZ** Specifies to which interface the rule should apply. If no rules are set or if no rule applies, the following default settings apply: – Remote access is permitted via *Internal, VPN*, and *Dial-in*. – Access via *External, External 2*, and *DMZ* is refused. Specify the access options according to your requirements. If you want to refuse access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as an action.
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, Reject has the same effect as Drop.) **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default settings).
Consolidated Imported Shares	**Enabled**	**No**: this network drive is not mirrored. **Yes**: this network drive is mirrored and made available.
	CIFS Share	Name of the network drive to be imported (created under *CIFS Integrity Monitoring >> Importable Shares >> Edit*).
	Exported in Subdirectory	The content of the included drive is located in this directory.

1 *External 2* and *Dial-in* are only for devices with a serial interface (see “Network >> Interfaces” on page 105).

Accessing the virtual network (CIFS Antivirus Scan Connector)

The virtual network drive provided by the mGuard for the CIFS Antivirus Scan Connector can be integrated in Windows Explorer. To do this, open the “Tools, Map Network Drive...” menu in Windows Explorer and enter the path using UNC notation.

This path is displayed under “CIFS Integrity Monitoring >> CIFS AV Scan Connector >> Accessible as”.

\\<External IP of MGUARD>\<Name of the exported share>
\\<Internal IP of MGUARD>\<Name of the exported share>

Example

\\10.1.66.49\exported-av-share

\\192.168.66.49\exported-av-share

Alternatively, you can enter the “net use” command in the command line. For further information, please refer to the Microsoft product information.

Notes

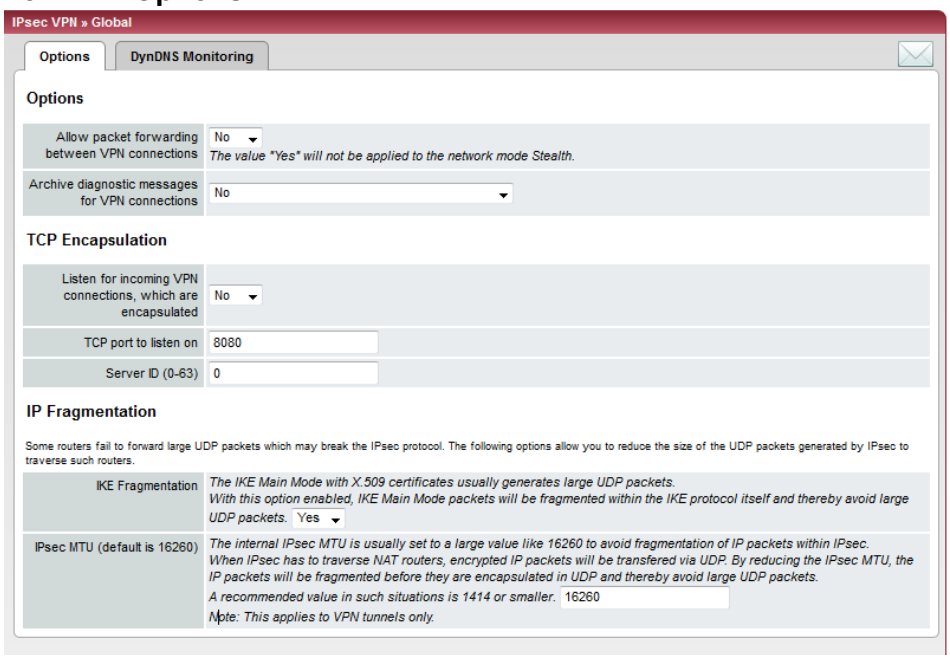
– DNS names can also be used instead of the IP address.
– The authorized network drive cannot be found using the browse or search function.
– The “Exported share's name” must always be added.
– Windows does not automatically display the authorized network drive upon connection of the mGuard.

10 IPsec VPN menu

This menu is **not** available on the **mGuard blade controller**.

10.1 IPsec VPN >> Global

10.1.1 Options


IPsec VPN » Global
Options
DynDNS Monitoring
Options
Allow packet forwarding between VPN connections
No
The value "Yes" will not be applied to the network mode Stealth.
Archive diagnostic messages for VPN connections
No
TCP Encapsulation
Listen for incoming VPN connections, which are encapsulated
No
TCP port to listen on
8080
Server ID (0-63)
0
IP Fragmentation
Some routers fail to forward large UDP packets which may break the IPsec protocol. The following options allow you to reduce the size of the UDP packets generated by IPsec to traverse such routers.
IKE Fragmentation
The IKE Main Mode with X.509 certificates usually generates large UDP packets.
With this option enabled, IKE Main Mode packets will be fragmented within the IKE protocol itself and thereby avoid large UDP packets.
Yes
IPsec MTU (default is 16260)
The internal IPsec MTU is usually set to a large value like 16260 to avoid fragmentation of IP packets within IPsec.
When IPsec has to traverse NAT routers, encrypted IP packets will be transfered via UDP. By reducing the IPsec MTU, the IP packets will be fragmented before they are encapsulated in UDP and thereby avoid large UDP packets.
A recommended value in such situations is 1414 or smaller.
16260
Note: This applies to VPN tunnels only.

IPsec VPN >> Global >> Options

Options

Allow packet forwarding between VPN connections

This option should only be set to **Yes** on an mGuard communicating between two different VPN partners.

To enable communication between two VPN partners, the local network of the communicating mGuard must be configured so that the remote networks containing the VPN partners are included. The opposite setup (local and remote network swapped round) must also be implemented for VPN partners (see “Remote” on page 265).

Yes is not supported in *Stealth* network mode.

No (default): VPN connections exist separately.

Yes: hub and spoke feature enabled: a control center diverts VPN connections to several branches that can also communicate with each other.

With a star VPN connection topology, mGuard partners can also exchange data with one another. In this case, it is recommended that the local mGuard consults CA certificates for the authentication of partners (see “Authentication” on page 269).

In the event of “hub and spoke”, 1:1 NAT of the partner is not supported.

Archive diagnostic messages for VPN connections:

The CMD contact is only available on the mGuard rs4000/rs2000, mGuard industrial rs

No/only when started via nph-vpn.cgi (or CMD input)

If errors occur when establishing VPN connections, the mGuard logging function can be used to find the source of the error based on corresponding entries (see *Logging >> Browse local logs* menu item). This option for error diagnostics is used as standard. Set this option to **No** (default) if it is sufficient.

Option **Only when started via nph-vpn.cgi (or CMD input):**

If the option of diagnosing VPN connection problems using the mGuard logging function is too impractical or insufficient, select this option. This may be the case if the following conditions apply:

IPsec VPN >> Global >> Options[...]

- In certain application environments, e.g., when the mGuard is “operated” by means of a machine controller via the CMD contact (*mGuard rs4000/rs2000 (3G)*, and *mGuard industrial rs* only), the option for a user to view the mGuard log file via the web-based user interface of the mGuard may not be available at all.
- When used remotely, it is possible that a VPN connection error can only be diagnosed after the mGuard is temporarily disconnected from its power source – which causes all the log entries to be deleted.
- The relevant log entries of the mGuard that could be useful may be deleted because the mGuard regularly deletes older log entries on account of its limited memory space.
- If an mGuard is being used as the central VPN partner, e.g., in a remote maintenance center as the gateway for the VPN connections of numerous machines, the messages regarding activity on the various VPN connections are logged in the same data stream. The resulting volume of the logging makes it time-consuming to find the information relevant to one error.

After archiving is enabled, relevant log entries about the operations involved in establishing VPN connections are archived in the non-volatile memory of the mGuard if the connections are established as follows:

- Via the CMD contact
- Via the CGI interface nph-vpn.cgi using the “synup” command (see Application Note: “How to use the CGI Interface”). (Application notes are available in the download area at www.innominate.com.)

Archived log entries are not affected by a restart. They can be downloaded as part of the support snapshot (*Support* >> *Advanced* menu item, *Snapshot* tab page). A snapshot provides your dealer's support team with additional options for more efficient troubleshooting than would be possible without archiving.

Archive diagnostic messages only upon failure: Yes/No	Only visible if archiving is enabled. If only log entries generated for failed connection attempts are to be archived, set this option to **Yes**. If set to **No**, all log entries will be archived.

TCP Encapsulation

This function is used to encapsulate data packets to be transmitted via a VPN connection in TCP packets. Without this encapsulation, under certain circumstances it is possible for VPN connections that important data packets belonging to the VPN connection may not be correctly transmitted due to interconnected NAT routers, firewalls or proxy servers, for example.

Firewalls, for example, may be set up to prevent any data packets of the UDP protocol from passing through or (incorrectly implemented) NAT routers may not manage the port numbers correctly for UDP packets.

TCP encapsulation avoids these problems because the packets belonging to the relevant VPN connection are encapsulated in TCP packets, i.e., they are hidden so that only TCP packets appear for the network infrastructure.

The mGuard may receive VPN connections encapsulated in TCP, even when it is positioned behind a NAT gateway in the network and thus cannot be reached by the VPN partner under its primary external IP address. To do this, the NAT gateway must forward the corresponding TCP port to the mGuard (see “Listen for incoming VPN connections, which are encapsulated” on page 251).

TCP encapsulation can only be used if an mGuard (Version 6.1 or later) is used at both ends of the VPN tunnel.

TCP encapsulation should only be used if required because connections are slowed down by the significant increase in the data packet overhead and by the correspondingly longer processing times.

If the mGuard is configured to use a proxy for HTTP and HTTPS in the *Network >> Proxy Settings* menu item, then this proxy is also used for VPN connections that use TCP encapsulation.

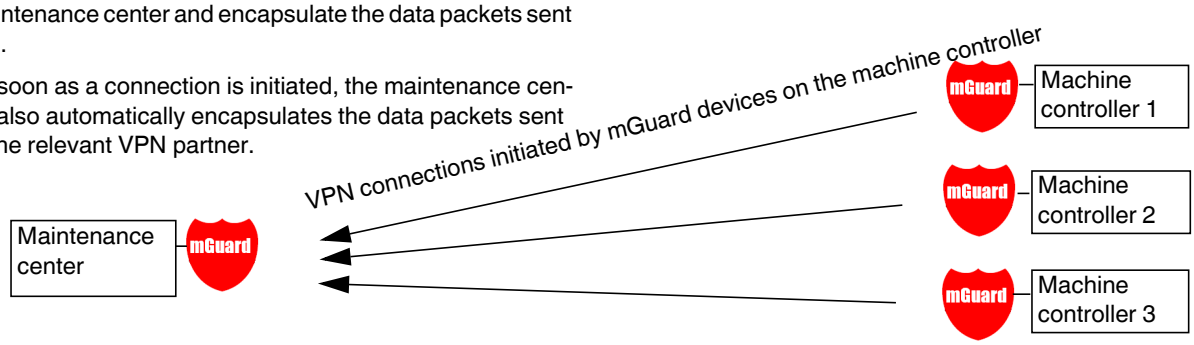
TCP encapsulation supports the *basic authentication* and *NTLM* authentication methods for the proxy.

For the TCP encapsulation to work through an HTTP proxy, the proxy must be named explicitly in the proxy settings (*Network >> Proxy Settings* menu item) (i.e., it must not be a transparent proxy) and this proxy must also understand and permit the HTTP method CONNECT.

TCP encapsulation does not work in connection with authentication via pre-shared key (PSK).

As devices in the TCP encapsulation, the mGuard devices for the machine controllers initiate VPN data traffic to the maintenance center and encapsulate the data packets sent to it.

As soon as a connection is initiated, the maintenance center also automatically encapsulates the data packets sent to the relevant VPN partner.



Maintenance center mGuard

Required basic settings

– **IPsec VPN** menu item, *Global*, *Options* tab page:
  Listen for incoming VPN connections, which are encapsulated: **Yes**
– *Connections* submenu,
  General tab page:
  Address of the partner's VPN gateway: **%any**
  Connection startup: **Wait**

mGuard **on machine controllers**

Required basic settings

– **IPsec VPN** menu item, *Global*, *Options* tab page:
  Listen for incoming VPN connections, which are encapsulated: **No**
– *Connections* submenu, *General* tab page:
  Address of the partner's VPN gateway: Fixed IP address or host name
  Connection startup: **Initiate** or **Initiate on traffic**
  Encapsulate the VPN traffic in TCP: **Yes**

Figure 10-1 TCP encapsulation in an application scenario with a maintenance center and machines maintained remotely via VPN connections

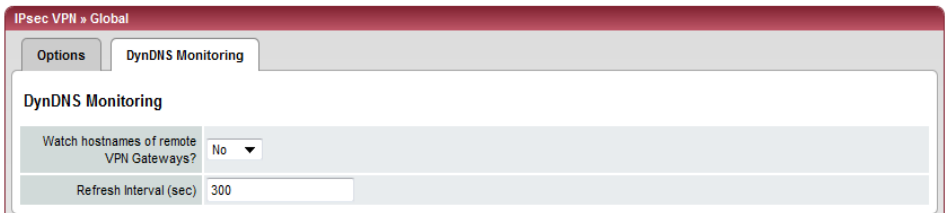
IPsec VPN >> Global >> Options

TCP Encapsulation	**Listen for incoming VPN connections, which are encapsulated**	Default setting: **No** Only set this option to Yes if the TCP Encapsulation function is used. Only then can the mGuard allow connection establishment with encapsulated packets. For technical reasons, the RAM (RAM) requirements increase with each interface that is used to listen out for VPN connections encapsulated in TCP. If multiple interfaces need to be used for listening, then the device must have at least 64 Mbytes RAM. The interfaces to be used for listening are determined by the mGuard according to the settings on the active VPN connections that have “%any” configured as the partner. The decisive setting is specified under “Interface to use for gateway setting %any”.

IPsec VPN >> Global >> Options[...]		
	TCP port to listen on	Number of the TCP port where the encapsulated data packets to be received arrive. The port number specified here must be the same as the one specified for the mGuard of the partner as the **TCP port of the server, which accepts the encapsulated connection** (*IPsec VPN >> Connections* menu item, Edit, *General* tab page). The following restriction applies: – The port to be used for listening must not be identical to a port that is being used for remote access (SSH, HTTPS or SEC-Stick).
	Server ID (0-63)	Usually, the default value **0** does not have to be changed. The numbers are used to differentiate between different control centers. A different number is only to be used in the following scenario: an mGuard connected upstream of a machine must establish connections to two or more different maintenance centers and their mGuard devices with TCP encapsulation enabled.
IP Fragmentation	**IKE Fragmentation:**	UDP packets can be oversized if an IPsec connection is established between the participating devices via IKE and certificates are exchanged. Some routers are not capable of forwarding large UDP packets if they are fragmented over the transmission path (e.g., via DSL in 1500-byte segments). Some faulty devices forward the first fragment only, resulting in connection failure. If two mGuard devices communicate with each other, it is possible to ensure at the outset that only small UDP packets are to be transmitted. This prevents packets from being fragmented during transmission, which can result in incorrect routing by some routers. If you want to use this option, set it to **Yes**. If this option is set to **Yes**, the setting only takes effect if the partner is an mGuard with installed firmware Version 5.1.0 or later. In all other cases, the setting has no effect, negative or otherwise.

IPsec VPN >> Global >> Options[...]		
	IPsec MTU (default is 16260)	The option for avoiding oversized IKE data packets, which cannot be routed correctly on the transmission path by faulty routers, can also be applied for IPsec data packets. In order to remain below the upper limit of 1500 bytes often set by DSL, it is recommended that a value of 1414 (bytes) be set. This also allows enough space for additional headers. If you want to use this option, specify a value lower than the default setting.

10.1.2 DynDNS Monitoring



For an explanation of DynDNS, see “DynDNS” on page 160.

IPsec VPN >> Global >> Options		
DynDNS Monitoring	**Watch hostnames of remote VPN Gateways?**	**Yes/No** If the mGuard has the address of a VPN partner in the form of a host name (see “Defining a new VPN connection/VPN connection channels” on page 255) and this host name is registered with a DynDNS service, then the mGuard can check the relevant DynDNS at regular intervals to determine whether any changes have occurred. If so, the VPN connection will be established to the new IP address.
	Refresh Interval (sec)	Default: 300

10.2 IPsec VPN >> Connections

Requirements for a VPN connection

A general requirement for a VPN connection is that the IP addresses of the VPN partners are known and can be accessed.

– mGuards provided in stealth network mode are preset to the “multiple clients” stealth configuration. In this mode, you need to configure a management IP address and default gateway if you want to use VPN connections (see Page 115). Alternatively, you can select a different stealth configuration than the “multiple clients” configuration or use another network mode.

– In order to successfully establish an IPsec connection, the VPN partner must support IPsec with the following configuration:
  – Authentication via pre-shared key (PSK) or X.509 certificates
  – ESP
  – Diffie-Hellman group 2 or 5
  – DES, 3DES or AES encryption
  – MD5, SHA-1 or SHA-2 hash algorithms
  – Tunnel or transport mode
  – Quick mode
  – Main mode
  – SA lifetime (1 second to 24 hours)

  If the partner is a computer running Windows 2000, the *Microsoft Windows 2000 High Encryption Pack* or at least *Service Pack 2* must be installed.

– If the partner is positioned downstream of a NAT router, the partner must support NAT-T. Alternatively, the NAT router must know the IPsec protocol (IPsec/VPN passthrough). For technical reasons, only IPsec tunnel connections are supported in both cases.

10.2.1 Connections

Lists all the VPN connections that have been defined.

Each connection name listed here can refer to an individual VPN connection or a group of VPN connection channels. You have the option of defining several tunnels under the transport and/or tunnel settings of the relevant entry.

You also have the option of defining new VPN connections, activating and deactivating VPN connections, changing (editing) the VPN connection or connection group properties, and deleting connections.

Defining a new VPN connection/VPN connection channels

- In the connections table, click on **Edit** to the right of the “(unnamed)” entry under “Name”.
- If the “(unnamed)” entry cannot be seen, open another row in the table.

Editing a VPN connection/VPN connection channels

- Click on **Edit** to the right of the relevant entry.

URL for starting, stopping, querying the status of a VPN connection

The following URL can be used to start and stop VPN connections or query their connection status, independently of their **Initial Mode** setting:

https://server/nph-vpn.cgi?name=verbindung&cmd=(up|down|status)

Example

wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

The *--no-check-certificate* option ensures that the HTTPS certificate on the mGuard does not undergo any further checking.

It may also be necessary to encode the password for the URL if it contains special characters.

A command like this relates to all connection channels that are grouped together under the respective name (in this example, *Athen*). This is the name that is listed under *IPsec VPN >> Connections >> Edit >> General* as *“A descriptive name for the connection”* . In the event of ambiguity, the URL call only affects the first entry in the list of connections.

It is not possible to communicate with the individual channels of a VPN connection. If individual channels are deactivated, they are not started. Starting and stopping in this way thus has no effect on the settings of the individual channels (i.e., the list under “Transport and Tunnel Settings”).

Starting and stopping a connection using a URL only makes sense if the connection is deactivated in the configuration or if **Connection startup** is set to “Stopped”. Otherwise, the mGuard (re)establishes the connection automatically.

If the status of a VPN connection is queried using the URL specified above, then the following responses can be expected:

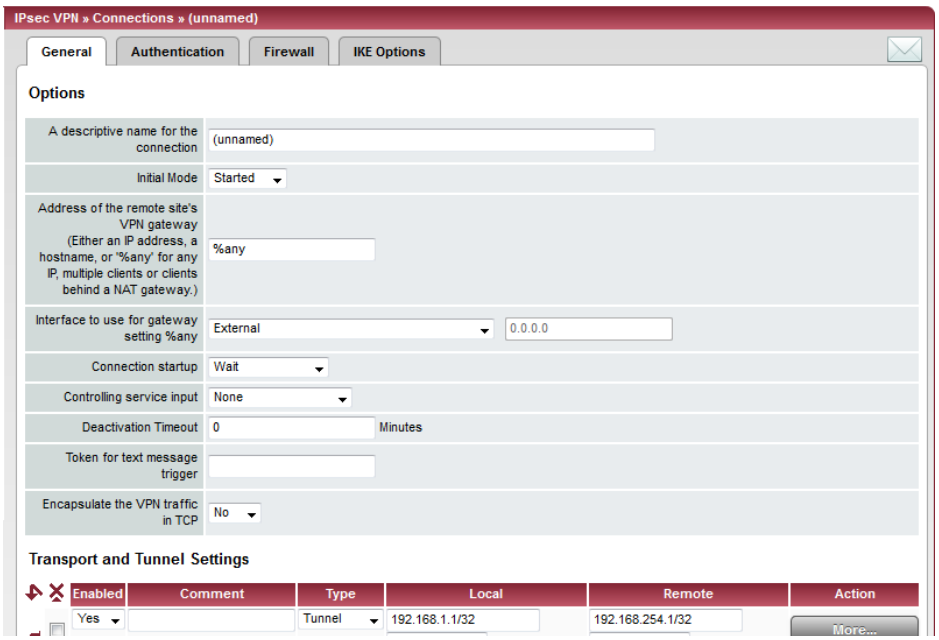
Table 10-1 Status of a VPN connection

Answer	Meaning
unknown	A VPN connection with this name does not exist.
void	The connection is inactive due to an error, e.g., the external network is down or the host name of the partner could not be resolved in an IP address (DNS). The response “void” is also issued by the CGI interface, even if no error occurred. If, for example, the VPN connection is deactivated according to the configuration (**No** set in column) and has not been enabled temporarily using the CGI interface or CMD contact.
ready	The connection is ready to establish channels or allow incoming queries regarding channel setup.
active	At least one channel has already been established for the connection.

Defining a VPN connection/VPN connection channels

Depending on the network mode of the mGuard, the following page appears after clicking on **Edit**.

10.2.2 General



IPsec VPN >> Connections >> Edit >> General		
Options	**A descriptive name for the connection**	The connection can be freely named/renamed. If several connection channels are defined under **Transport and Tunnel Settings**, then this name applies to the entire set of VPN connection channels grouped under this name. Similarities between VPN connection channels: – Same authentication method, as specified on the *Authentication* tab page (see “Authentication” on page 269) – Same firewall settings – Same IKE options set
	Initial Mode	**Started/Disabled/Stopped** The “Disabled” setting deletes the VPN connection. The other two settings determine the status of the VPN connection when restarting the connection or booting. With Version 8.0 or later, the VPN connections can be started or stopped via a button on the web interface, via text message or the nph-vpn.cgi script.
	Address of the remote site's VPN gateway	(An IP address, host name or **%any** for several partners or partners downstream of a NAT router)

Address of the remote site's VPN gateway

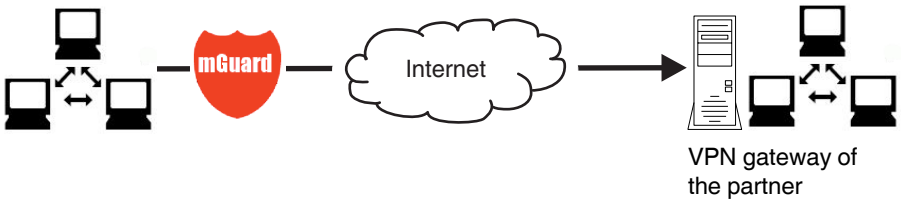


Figure 10-2 The address of the transition to the private network where the remote communication partner is located.

– If the mGuard should actively initiate and establish the connection to the remote partner, specify the IP address or host name of the partner here.
– If the VPN gateway of the partner does not have a fixed and known IP address, the DynDNS service (see glossary) can be used to simulate a fixed and known address.
– If the mGuard should be ready to allow a connection to the local mGuard that was actively initiated and established by a remote partner with any IP address, specify **%any**.
  This setting should also be selected for a VPN star configuration if the mGuard is connected to the control center.
  The mGuard can then be "called" by a remote partner if this partner has been dynamically assigned its IP address (by the Internet service provider), i.e., it has an IP address that changes. In this scenario, you may only specify an IP address if the remote "calling" partner also has a fixed and known IP address.

%any can only be used together with the authentication method using X.509 certificates.

If locally stored CA certificates are to be used to authenticate the partner, the address of the VPN gateway of the partner can be specified explicitly (by means of an IP address or host name) or by **%any**. If it is specified using an explicit address (and not by "%any"), then a VPN identifier (see "VPN Identifier" on page 272) must be specified.

%any must be selected if the partner is located downstream of a NAT gateway. Otherwise, the renegotiation of new connection keys will fail on initial contact.

If **TCP Encapsulation** is used (see "TCP Encapsulation" on page 250): a fixed IP address or a host name must be specified if this mGuard is to initiate the VPN connection and encapsulate the VPN data traffic.

If this mGuard is installed upstream of a maintenance center to which multiple remote mGuard devices establish VPN connections and transmit encapsulated data packets, **%any** must be specified for the VPN gateway of the partner.

IPsec VPN >> Connections >> Edit >> General		
Options	**Interface to use for gateway setting %any**	**Internal, External, External 2, Dial-in, DMZ, Implicitly selected by the IP address specified to the right** *External 2* and *Dial-in* are only for devices with a serial interface, see “Network >> Interfaces” on page 105. Selection *of the* **Internal** option is not permitted in Stealth mode. This interface setting is only considered when “%any” is entered as the address of the VPN gateway on the partner. In this case, the interface of the mGuard through which it answers and permits requests for the establishment of this VPN connection is set here. The VPN connection can be established through the LAN and WAN port in all Stealth modes when **External** is selected. The interface setting allows encrypted communication to take place over a specific interface for VPN partners without a known IP address. If an IP address or host name is entered for the partner, then this is used for the implicit assignment to an interface. The mGuard can be used as a “single-leg router” in Router mode when **Internal** is selected, as both encrypted and decrypted VPN traffic for this VPN connection is transferred over the internal interface. IKE and IPsec data traffic is only possible through the primary IP address of the individual assigned interface. This also applies to VPN connections with a specific partner. **DMZ** can only be selected in Router mode. Here, VPN connections can be established to hosts in the DMZ and IP packets can be routed from the DMZ in a VPN connection. **Implicitly selected by the IP address specified to the right**: an IP address is used instead of a dedicated interface.

IPsec VPN >> Connections >> Edit >> General [...]

Connection startup

Initiate/Initiate on traffic/Wait

Initiate

The mGuard initiates the connection to the partner. In the *Address of the remote site's VPN gateway* field (see above), the fixed IP address of the partner or its name must be entered.

Initiate on traffic

The connection is initiated automatically when the mGuard sees that the connection should be used.

(Can be selected for all operating modes of the mGuard (*Stealth, Router*, etc.).)

Wait

The mGuard is ready to allow the connection to the mGuard that a remote partner actively initiates and establishes.

If %any is entered under *Address of the remote site's VPN gateway*, Wait must be selected.

Controlling service input

Only available with the mGuard rs4000/rs2000 3G, mGuard rs4000/rs2000, mGuard industrial rs.

None/Service input CMD 1-3

The VPN connection can be switched via a connected push button/switch.

The push button/switch must be connected to one of the service contacts (CMD 1-3).

If starting and stopping the VPN connection via the CMD contact is enabled, only the CMD contact is authorized to do this, i.e., this means that setting this option to Enabled for the entire VPN connection has no effect.

However, if a button is connected to the CMD contact (instead of a switch – see below), the connection can also be established and disconnected using the CGI script command nph-vpn.cgi or via a text message, which has the same rights.

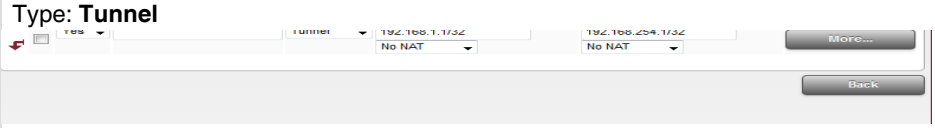
If a VPN connection is controlled via a VPN switch, then VPN redundancy cannot be activated.

IPsec VPN >> Connections >> Edit >> General [...]	
Use inverted control logic	Inverts the behavior of the connected switch. If the switching service input is configured as an on/off switch, it can activate one VPN connection and deactivate another.
Deactivation Timeout	Time, after which the VPN connection is deactivated, if it has been started via a text message, switch, button, nph-vpn.cgi or the web interface. VPN connections which have been started by an explicit request via an application are not affected. Time in minutes (0 to 10000, approx. 1 week) 0 means the setting is switched off. VPN connections which have been started via a text message, switch, button, nph-vpn.cgi or the web interface are aborted once this time has elapsed.
Token for text message trigger	Only available with the mGuard rs4000/rs2000 3G. Incoming text messages can be used to start or stop VPN connections. The text message must contain the command “vpn/start” or “vpn/stop” followed by the token.
Encapsulate the VPN traffic in TCP	**Yes/No (default: No)** If the **TCP Encapsulation** function is used (see “TCP Encapsulation” on page 250), only set this option to **Yes** if the mGuard is to encapsulate its own outgoing data traffic for the VPN connection it initiated. In this case, the number of the port where the partner receives the encapsulated data packets must also be specified. When **Yes** is selected, the mGuard will not attempt to establish the VPN connection using standard IKE encryption (UDP port 500 and 4500). Instead, the connection is always encapsulated using TCP.
TCP-Port of the server, which accepts the encapsulated connection (Only visible if “Encapsulate the VPN traffic in TCP” is set to **Yes**.)	Default: **8080**. Number of the port where the encapsulated data packets are received by the partner. The port number specified here must be the same as the one specified for the mGuard of the partner under **TCP port to listen on** (*IPsec VPN >> Global >> Options* menu item). **If TCP Encapsulation is used (see Page 250):** – If the mGuard is to establish a VPN connection to a maintenance center and encapsulate the data traffic there: – **Initiate** or **Initiate on traffic** must be specified. – If the mGuard is installed at a maintenance center to which mGuard devices establish a VPN connection: – **Wait** must be specified.

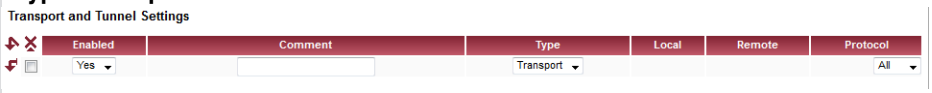
IPsec VPN >> Connections >> Edit >> General [...]

Transport and Tunnel Settings

Type: **Tunnel**



Type: Transport



Enabled

Yes/No

Specify whether the connection channel should be active (Yes) or not (No).

Comment

Freely selectable comment text. Can be left empty.

Protocol

All means TCP, UDP, ICMP, and other IP protocols

Type

The following can be selected:

– Tunnel (network ↔ network)

– Transport (host ↔ host)

Tunnel (network ↔ network)

This connection type is suitable in all cases and is also the most secure. In this mode, the IP datagrams to be transmitted are completely encrypted and are, with a new header, transmitted to the VPN gateway of the partner – the “tunnel end”. The transmitted datagrams are then decrypted and the original datagrams are restored. These are then forwarded to the destination computer.

Transport (host ↔ host)

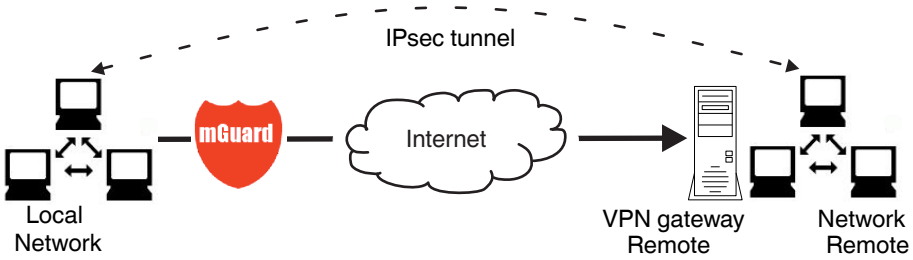
For this type of connection, only the data of the IP packets is encrypted. The IP header information remains unencrypted.

When you switch to *Transport*, the following fields (apart from Protocol) are hidden as these parameters are omitted.

IPsec VPN >> Connections >> Edit >> General [...]

Local/Remote - for *Tunnel* connection type

Define the network areas for both tunnel ends under **Local** and **Remote**.



Type: Tunnel

No NAT/1:1-NAT/Masquerade

It is possible to translate the IP addresses of devices located at the respective end of the VPN tunnel.

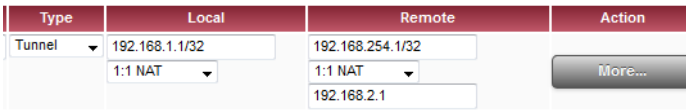
No NAT: NAT is not performed.

Local

Here, specify the address of the network or computer which is connected locally to the mGuard.

Type: Tunnel, Local

1:1 NAT



With 1:1 NAT, the IP addresses of devices at the local end of the tunnel are exchanged so that each individual address is translated into another specific address. It is not translated into an IP address that is identical for all devices (as is the case with **Masquerading**).

If local devices transmit data packets, only those data packets are considered which:

– Are actually encrypted by the mGuard (the mGuard only forwards packets via the VPN tunnel if they originate from a trustworthy source).
– Originate from a source address within the network which is defined here.
– Have their destination address in the network *of the partner* if 1:1 NAT is not set there for the partner.

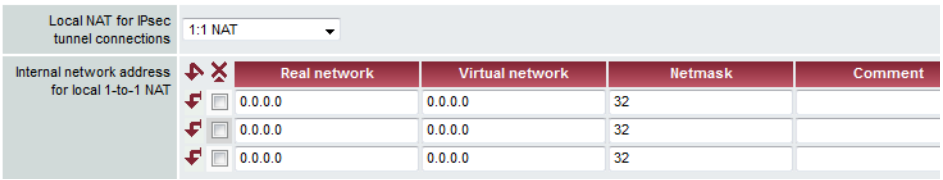
The data packets of local devices are assigned a source address according to the address set under *Local* and are transmitted via the VPN tunnel.

After clicking on the "**More**" button, 1:1 NAT rules can be specified for each VPN tunnel for local devices. In this way, an IP range that is distributed over a wide network can be gathered and sent through a narrow tunnel.

IPsec VPN >> Connections >> Edit >> General [...]

Type: Tunnel, Local, 1:1-NAT, „More“ button

Local NAT



Real network — Configures the “From IP” address for 1:1 NAT.

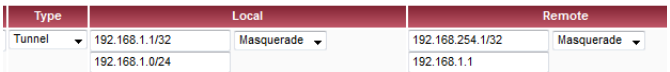
Virtual Network — Configures the translated IP address for 1:1 NAT.

Netmask — The subnet mask as a value between 1 and 32 for the real and virtual network address (see also “CIDR (Classless Inter-Domain Routing)” on page 24).

Comment — Can be filled with appropriate comments.

Local 1:1 networks must be specified in ascending order, beginning with the smallest network up to the largest network.

Type: Tunnel, Local **Masquerade**



If local devices transmit data packets, only those data packets are considered which:

– Are actually encrypted by the mGuard (the mGuard only forwards packets via the VPN tunnel if they originate from a trustworthy source).
– Originate from a source address within the network which is defined here.
– Have their destination address in the network *of the partner* if 1:1 NAT is not set for the *partner* NAT.

Only one IP address (subnet mask /32) is permitted as the VPN network for this setting. The network to be masqueraded is translated to this IP address.

The data packets are then transmitted via the VPN tunnel. Masquerading changes the source address (and source port). The original addresses are recorded in an entry in the Conntrack table.

Where response packets are received via the VPN tunnel and there is a matching entry in the Conntrack table, these packets have their destination address (and destination port) written back to them.

IPsec VPN >> Connections >> Edit >> General [...]

Remote

Here, specify the address of the network or computer which is located downstream of the remote VPN gateway.

Type: Tunnel, Remote

1:1 NAT

With 1:1 NAT, the IP addresses of devices of the tunnel partner are exchanged so that each individual address is translated into another specific address. It is not translated into an IP address that is identical for all devices (as is the case with **Masquerading**).

If local devices transmit data packets, only those data packets are considered which:

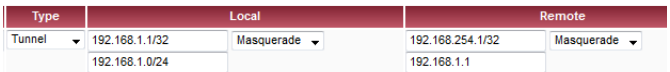
– Are actually encrypted by the mGuard (the mGuard only forwards packets via the VPN tunnel if they originate from a trustworthy source).

– Have a source address within the network which is defined here under Local.

The data packets are assigned a destination address from the network that is set under Remote. If necessary, the source address is also replaced (see Local). The data packets are then transmitted via the VPN tunnel.

Type: Tunnel, Remote

Masquerade



Only one IP address (subnet mask /32) is permitted as the VPN network for this setting. The network to be masqueraded is translated to this IP address.

The data packets are then transmitted via the VPN tunnel. Masquerading changes the source address (and source port). The original addresses are recorded in an entry in the Conntrack table.

Where response packets are received via the VPN tunnel and there is a matching entry in the Conntrack table, these packets have their destination address (and destination port) written back to them.

Tunnel settings IPsec/L2TP

If clients should connect via the mGuard by IPsec/L2TP, activate the L2TP server and make the following entries in the fields specified below:

– **Type**: Transport
– **Protocol**: UDP
– **Local:** %all
– **Remote:** %all
– **PFS**: No (“Perfect Forward Secrecy (PFS)” on page 281)

Specifying a default route over the VPN

Address 0.0.0.0/0 specifies a *default route over the VPN*.

With this address, all data traffic where no other tunnel or route exists is routed through this VPN tunnel.

A default route over the VPN should only be specified for a single tunnel.

In *Stealth* mode, a *default route over the VPN* cannot be used.

Option following installation of a VPN tunnel group license

If *Address of the remote site's VPN gateway* is specified as **%any**, it is possible that there are many mGuard devices or many networks on the remote side.

A very large address area is then specified in the **Remote** field for the local mGuard. A part of this address area is used on the remote mGuard devices for the network specified for each of them under **Local**.

This is illustrated as follows: the entries in the **Local** and **Remote** fields for the local and remote mGuard devices could be made as follows:

Local mGuard			Remote mGuard **A**	
Local	Remote		Local	Remote
10.0.0.0/8	10.0.0.0/8	>	10.1.7.0/24	10.0.0.0/8
			Remote mGuard **B**	
			Local	Remote
		>	10.3.9.0/24	10.0.0.0/8
			Etc.	

In this way, by configuring a single tunnel, you can establish connections for a number of peers.

To use this option, the *VPN tunnel group license* must be installed first. The device must be restarted in order to use this installed license.

Masquerade

Can only be used for *Tunnel* VPN type.

Example

A control center has one VPN tunnel each for a large number of branches. One local network with numerous computers is installed in each of the branches, and these computers are connected to the control center via the relevant VPN tunnel. In this case, the address area could be too small to include all the computers at the various VPN tunnel ends.

Masquerading solves this problem:

The computers connected in the network of a branch appear under a single IP address by means of masquerading for the VPN gateway of the control center. In addition, this enables the local networks in the various branches to all use the same network address locally. Only the branch can establish VPN connections to the control center.

Network address for masquerading

Specify the IP address area, for which masquerading is used.

The sender address in the data packets sent by a computer via the VPN connection is only replaced by the address specified in the **Local** field (see above) if this computer has an IP address from this address area.

The address specified in the **Local** field must have the subnet mask "/32" to ensure that only one IP address is signified.

Masquerading can be used in the following network modes: Router, PPPoE, PPTP, Modem, Built-in Modem, Built-in mobile network modem, and Stealth (only "multiple clients" in Stealth mode).

Modem/Built-in modem/Built-in mobile network modem is not available for all mGuard models (see "Network >> Interfaces" on page 105).

For IP connections via a VPN connection with active masquerading, the firewall rules for outgoing data in the VPN connection are used for the original source address of the connection.

1:1 NAT

With 1:1 NAT in VPN, it is still possible to enter the network addresses actually used to specify the tunnel beginning and end, independently of the tunnel parameters agreed with the partner:

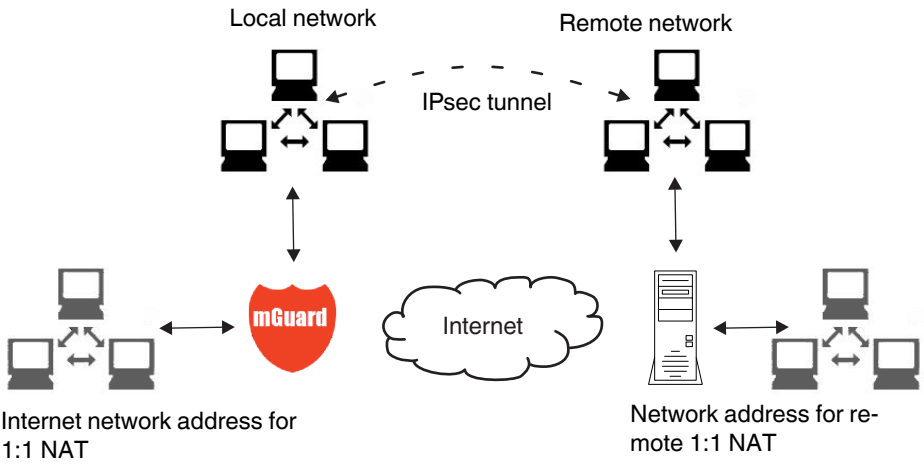
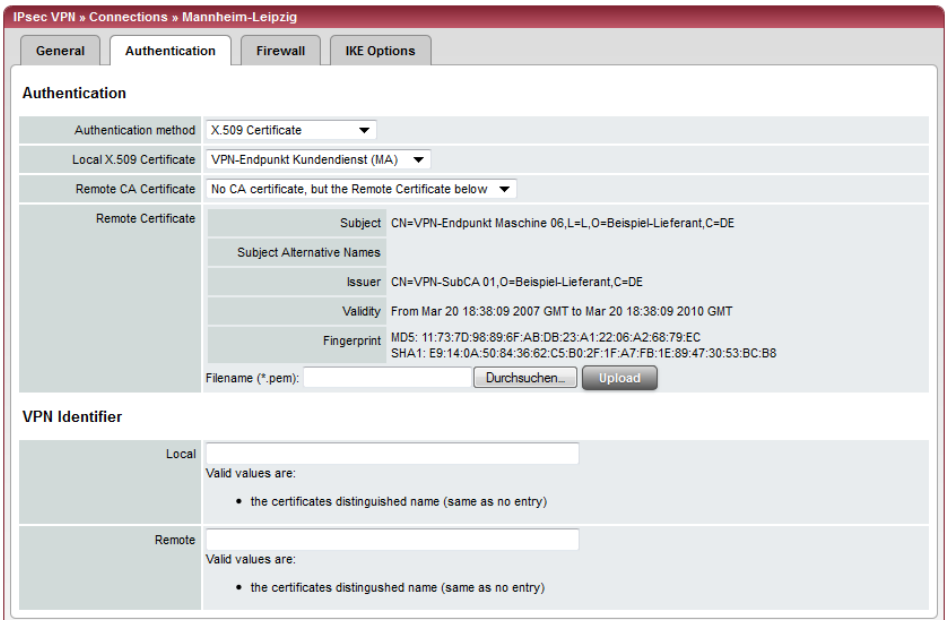


Figure 10-3 1:1 NAT

10.2.3 Authentication



IPsec VPN >> Connections >> Edit >> Authentication

Authentication

Authentication method

There are two options:

– X.509 Certificate (default)

– Pre-shared Secret (PSK)

Depending on the chosen method, the page contains different setting options.

Authentication method: X.509 Certificate

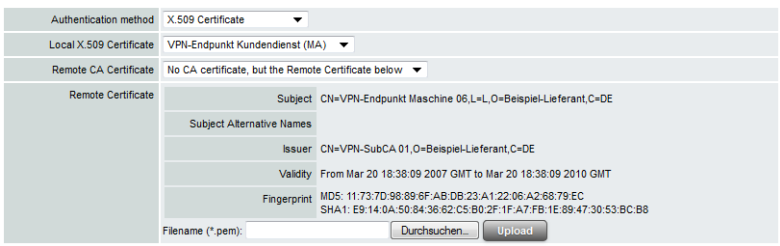
This method is supported by most modern IPsec implementations. With this option, each VPN device has a secret private key and a public key in the form of an X.509 certificate, which contains further information about the certificate's owner and the certification authority (CA).

The following must be specified:

– How the mGuard authenticates itself to the partner

– How the mGuard authenticates the remote partner

How the mGuard authenticates itself to the partner



IPsec VPN >> Connections >> Edit >> Authentication

Local X.509 Certificate

Specifies which machine certificate the mGuard uses as authentication to the VPN partner.

Select one of the machine certificates from the selection list.

The selection list contains the machine certificates that have been loaded on the mGuard under the *Authentication >> Certificates* menu item.

If *None* is displayed, a certificate must be installed first. *None* must not be left in place, as this results in no X.509 authentication.

How the mGuard authenticates the remote partner

The following definition relates to how the mGuard verifies the authenticity of the VPN remote partner.

The table below shows which certificates must be provided for the mGuard to authenticate the VPN partner if the VPN partner shows one of the following certificate types when a connection is established:

– A machine certificate signed by a CA
– A self-signed machine certificate

For additional information about the table, see "Authentication >> Certificates" on page 190.

Authentication for VPN

The partner shows the following:	Machine certificate, **signed by CA**	Machine certificate, **self-signed**
The mGuard authenticates the partner using:	⇕	⇕
	Remote certificate Or all CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner	Remote certificate

According to this table, the certificates that must be provided are the ones the mGuard uses to authenticate the relevant VPN partner.

Requirement

The following instructions assume that the certificates have already been correctly installed on the mGuard (see*"Authentication >> Certificates" on page 190*, apart from the remote certificate).

If the use of revocation lists (CRL checking) is activated under the *Authentication >> Certificates, Certificate settings* menu item, each certificate signed by a CA that is "shown" by the VPN partner is checked for revocations. This excludes locally configured (imported) remote certificates.

Remote CA Certificate

Self-signed machine certificate

If the VPN partner authenticates itself with a **self-signed** machine certificate:

- Select the following entry from the selection list:
  "No CA certificate, but the Remote Certificate below"
- Install the remote certificate under *Remote Certificate* (see "Installing the remote certificate" on page 271).

It is not possible to reference a remote certificate loaded under the *Authentication >> Certificates* menu item.

Machine certificate signed by the CA

If the VPN partner authenticates itself with a machine certificate **signed by a CA**:

It is possible to authenticate the machine certificate shown by the partner as follows:

– Using CA certificates
– Using the corresponding remote certificate

Authentication using a CA certificate:

Only the CA certificate from the CA that signed the certificate shown by the VPN partner should be referenced here (selection from list). The additional CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner must be installed on the mGuard under the *Authentication >> Certificates* menu item.

The selection list contains all CA certificates that have been loaded on the mGuard under the *Authentication >> Certificates* menu item.

The other option is "*Signed by any trusted CA*".

With this setting, all VPN partners are accepted, providing that they log in with a signed CA certificate issued by a recognized certification authority (CA). The CA is recognized if the relevant CA certificate and all other CA certificates have been loaded on the mGuard. These then form the chain to the root certificate together with the certificates shown.

Authentication using the corresponding remote certificate:

- Select the following entry from the selection list:
  "No CA certificate, but the Remote Certificate below"
- Install the remote certificate under *Remote Certificate* (see "Installing the remote certificate" on page 271).

It is not possible to reference a remote certificate loaded under the *Authentication >> Certificates* menu item.

Installing the remote certificate

The remote certificate must be configured if the VPN partner is to be authenticated using a remote certificate.

To import a certificate, proceed as follows:

Requirement: The certificate file (file name extension: *.pem, *.cer or *.crt) is saved on the connected computer.

- Click on **Browse...** to select the file.
- Click on **Upload**.
  The contents of the certificate file are then displayed.

IPsec VPN >> Connections >> Edit >> Authentication

VPN Identifier

Authentication method: CA certificate

The following explanation applies if the VPN partner is authenticated using CA certificates.

VPN gateways use the VPN identifier to detect which configurations belong to the same VPN connection.

If the mGuard consults CA certificates to authenticate a VPN partner, then it is possible to use the VPN identifier as a filter.

- Make a corresponding entry in the *Remote* field.

Local

Default: empty field

The local VPN identifier can be used to specify the name the mGuard uses to identify itself to the partner. It must match the data in the machine certificate of the mGuard.

Valid values:

– Empty, i.e., no entry (default). The “Subject” entry (previously *Distinguished Name*) in the machine certificate is then used.
– The “Subject” entry in the machine certificate.
– One of the *Subject Alternative Names*, if they are listed in the certificate. If the certificate contains *Subject Alternative Names*, these are specified under “Valid values are”. These can include IP addresses, host names with “@” prefix or e-mail addresses.

Remote

Specifies what must be entered as a subject in the machine certificate of the VPN partner for the mGuard to accept this VPN partner as a communication partner.

It is then possible to limit or enable access by VPN partners, which the mGuard would accept in principle based on certificate checks, as follows:

– Limited access to certain *subjects* (i.e., machines) and/or to *subjects* that have certain attributes or
– Access enabled for all *subjects*

(See “Subject, certificate” on page 360.)

“Distinguished Name” was previously used instead of “Subject”.

IPsec VPN >> Connections >> Edit >> Authentication[...]

Access enabled for all subjects:

If the *Remote* field is left empty, then any subject entries are permitted in the machine certificate shown by the VPN partner. It is then no longer necessary to identify or define the subject in the certificate.

Limited access to certain subjects:

In the certificate, the certificate owner is specified in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an object identifier (e.g., 132.3.7.32.1) or, more commonly, as an abbreviation with a corresponding value.

Example: CN=VPN endpoint 01, O=Smith and Co., C=US

If certain subject attributes have very specific values for the acceptance of the VPN partner by the mGuard, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the ***** (asterisk) wildcard.

Example: CN=*, O=Smith and Co., C=US (with or without spaces between attributes)

In this example, the attributes “O=Smith and Co.” and “C=US” should be entered in the certificate that is shown under “Subject”. It is only then that the mGuard would accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have any value.

Please note the following when setting a subject filter:

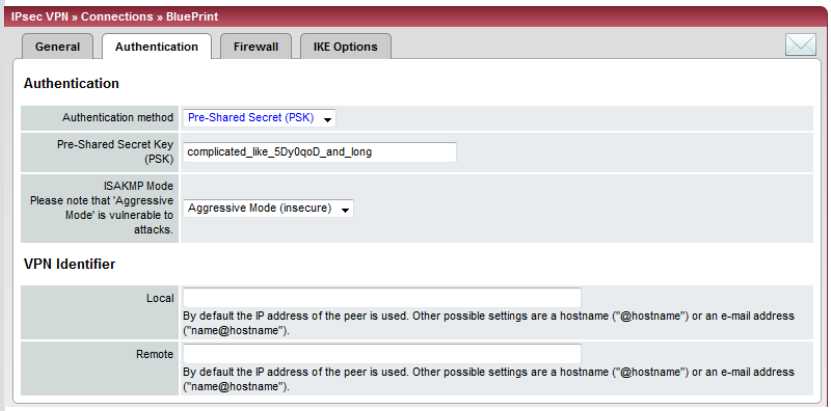
The number and the order of the attributes must correspond to that of the certificates for which the filter is used

Please note this is case-sensitive.

IPsec VPN >> Connections >> Edit >> Authentication[...]

Authentication

Authentication method: Pre-Shared Secret (PSK)


IPsec VPN » Connections » BluePrint
General
Authentication
Firewall
IKE Options
Authentication
Authentication method
Pre-Shared Secret (PSK)
Pre-Shared Secret Key (PSK)
complicated_like_5Dy0qoD_and_long
ISAKMP Mode
Please note that 'Aggressive Mode' is vulnerable to attacks.
Aggressive Mode (insecure)
VPN Identifier
Local
By default the IP address of the peer is used. Other possible settings are a hostname ("@hostname") or an e-mail address ("name@hostname").
Remote
By default the IP address of the peer is used. Other possible settings are a hostname ("@hostname") or an e-mail address ("name@hostname").

This method is mainly supported by older IPsec implementations. In this case, both sides of the VPN authenticate themselves using the same PSK.

To make the agreed key available to the mGuard, proceed as follows:

- Enter the agreed string in the **Pre-Shared Secret Key (PSK)** entry field.

To achieve security comparable to that of 3DES, the string should consist of around 30 randomly selected characters, and should include upper and lower case characters and digits.

When PSK is used together with the “Aggressive Mode (insecure)” setting, a fixed Diffie-Hellman algorithm must be selected under IKE Options for the initiator of the connection.

When PSK is used together with the “Aggressive Mode (insecure)” setting, all Diffie-Hellman algorithms should be selected under IKE Options for the responder of the connection.

When using a fixed Diffie-Hellman algorithm, it must be the same for all connections using the “Aggressive Mode (insecure)” setting.

IPsec VPN >> Connections >> Edit >> Authentication[...]

ISAKMP Mode

Main Mode (secure)

In main mode, the party wishing to establish the connection (initiator) and the responder negotiate an ISAKMP SA.

We recommend using certificates in main mode.

Aggressive Mode (insecure)

Encryption for aggressive mode is not as secure as for main mode. The use of this mode can be justified if the responder does not know the initiator's address in advance, and both parties wish to use pre-shared keys for authentication. Another reason may be the wish for faster connection establishment if the responder's principles are sufficiently known, e.g., an employee wishing to access the company network.

Requirement:

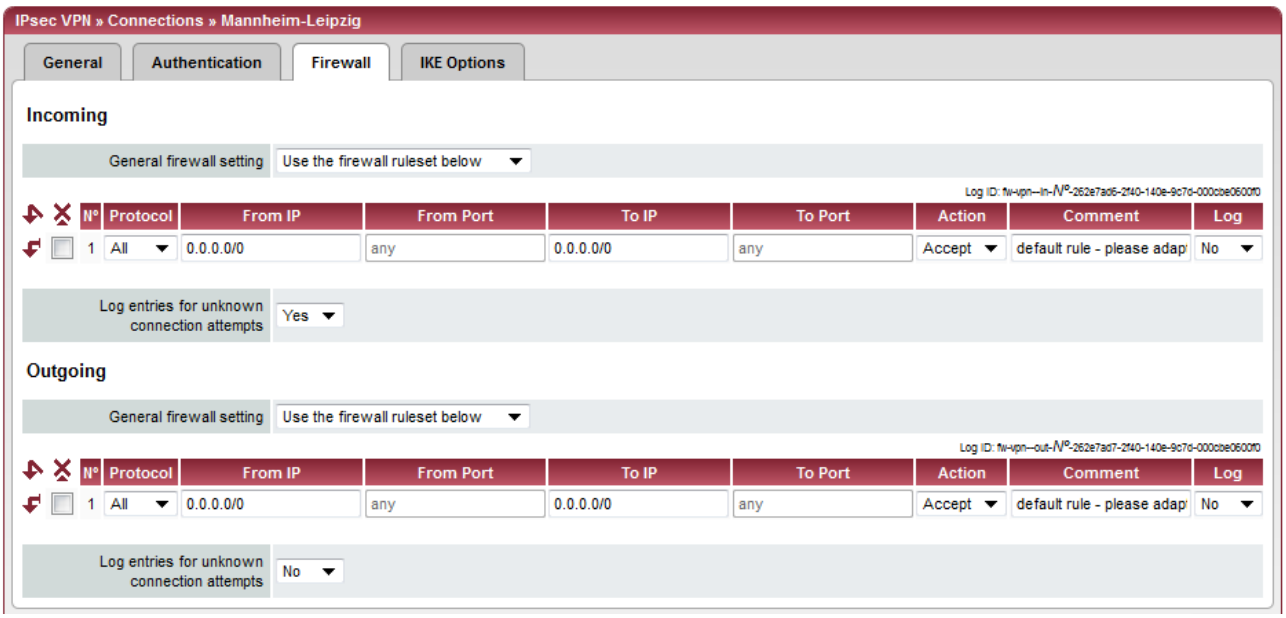
- Cannot be used together with the redundancy function.
- The same mode must be used between peers.
- If two VPN clients downstream of the same NAT gateway establish the same connection to a VPN gateway, they must use the same PSK. As an alternative, the VPN gateway must provide each client with a different VPN identifier for the partner, which is set as the local VPN identifier on the client.

VPN gateways use the *VPN Identifier* to detect which configurations belong to the same VPN connection.

The following entries are valid for PSK:

- Empty (IP address used by default)
- An IP address
- A host name with “@” prefix (e.g., “@vpn1138.example.com”)
- An e-mail address (e.g., “piepiorra@example.com”)

10.2.4 Firewall



Incoming/outgoing firewall

While the settings made under the *Network Security* menu item only relate to non-VPN connections (see above under “Network Security menu” on page 205), the settings here only relate to the VPN connection defined on these tab pages.

If multiple VPN connections have been defined, you can limit the outgoing or incoming access individually for each connection. Any attempts to bypass these restrictions can be logged.

By default, the VPN firewall is set to allow all connections for this VPN connection.

However, the extended firewall settings defined and explained above apply independently for each individual VPN connection (see “Network Security menu” on page 205, “Network Security >> Packet Filter” on page 205, “Advanced” on page 216).

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

In *Stealth* mode, the actual IP address used by the client should be used in the firewall rules, or it should be left at 0.0.0.0/0, as only one client can be addressed through the tunnel.

If the *Allow packet forwarding between VPN connections* option is set to **Yes** on the *Global* tab page, the rules under **Incoming** are used for the incoming data packets to the mGuard, and the rules under **Outgoing** are applied to the outgoing data packets.

If the outgoing data packets are included in the same connection definition (for a defined VPN connection group), then the firewall rules for **Incoming** and **Outgoing** for the same connection definition are used.

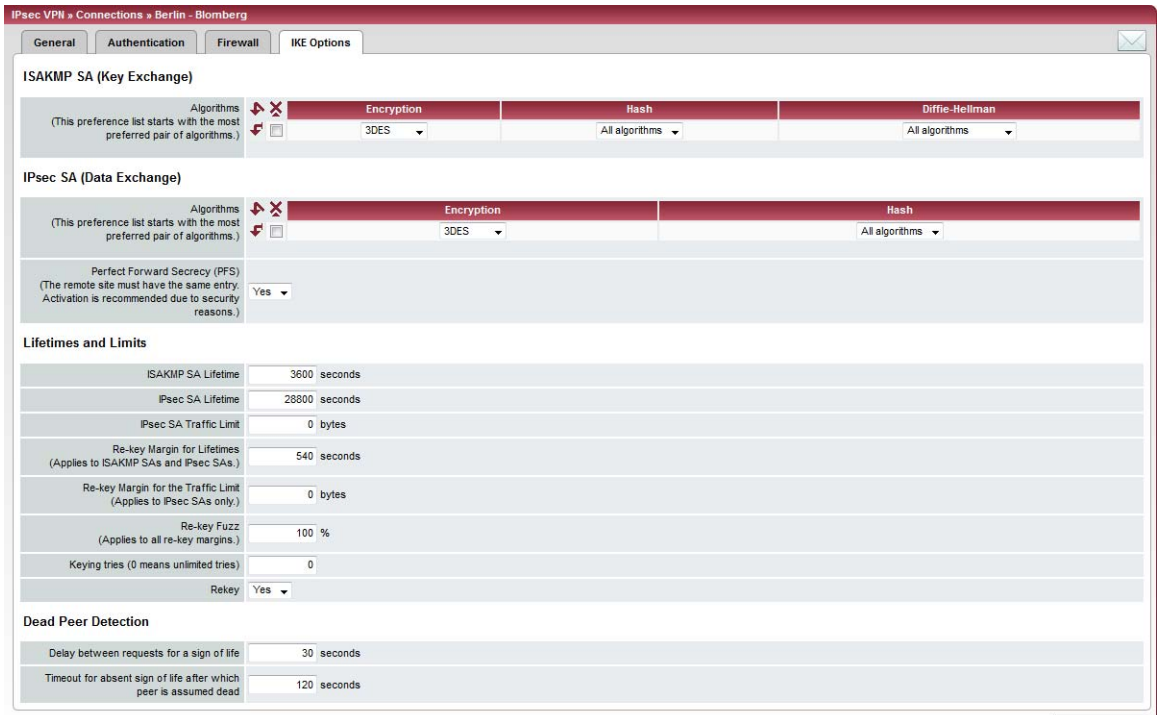
If a different VPN connection definition applies to the outgoing data packets, the firewall rules for **Outgoing** for this other connection definition are used.

If the mGuard has been configured to forward SSH connection packets (e.g., by permitting a SEC-Stick hub & spoke connection), existing VPN firewall rules are not applied. This means, for example, that packets of an SSH connection are sent via a VPN tunnel despite the fact that this is prohibited by its firewall rules.

IPsec VPN >> Connections >> Edit >> Firewall		
Incoming	**General firewall setting**	**Allow all incoming connections**: the data packets of all incoming connections are allowed. **Drop all incoming connections**: the data packets of all incoming connections are discarded. **Accept Ping only:** the data packets of all incoming connections are discarded, except for ping packets (ICMP). **Use the firewall ruleset below**: displays further setting options. This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.
	The following settings are only visible if "**Use the firewall ruleset below**" is set.	
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols
	From IP/To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 24). **Incoming:** – From IP: the IP address in the VPN tunnel – To IP: the 1:1 NAT address or the actual address **Outgoing**: – From IP: the 1:1 NAT address or the actual address – To IP: the IP address in the VPN tunnel

IPsec VPN >> Connections >> Edit >> Firewall		
	From Port/To Port	(Only evaluated for TCP and UDP protocols.) – **any** refers to any port. – **startport:endport** (e.g., 110:120) refers to a port area. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, Reject has the same effect as Drop.) **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default settings).
	Log entries for unknown connection attempts	When set to **Yes**, all connection attempts that are not covered by the rules defined above are logged.
Outgoing	The explanation provided under “Incoming” also applies to “Outgoing”.	

10.2.5 IKE Options



IPsec VPN >> Connections >> Edit >> IKE Options		
ISAKMP SA (Key Exchange)	**Algorithms**	Decide on which encryption method should be used with the administrator of the partner. **Encryption** 3DES-168 is the most commonly used method and is therefore set by default. Fundamentally, the following applies: the more bits an encryption algorithm has (specified by the appended number), the more secure it is. The relatively new AES-256 method is therefore the most secure, however it is still not used that widely. The longer the key, the more time-consuming the encryption procedure. However, this does not affect the mGuard as it uses a hardware-based encryption technique. Nevertheless, this aspect may be of significance for the partner. The algorithm designated as “Null” does not contain encryption. **Hash** Leave this set to *All algorithms*. It then does not matter whether the partner is operating with MD5, SHA-1, SHA-256, SHA-384 or SHA-512. The encryption algorithms SHA-256 and SHA-512 are supported by all mGuard devices. However, not all mGuard devices accelerate the algorithms via hardware. The *mGuard centerport* supports and does not require hardware acceleration. Only the mGuard smart^2 also accelerates SHA-256 via hardware. On the other mGuard devices, MD5 and SHA1 are accelerated with hardware. **Diffie-Hellman** The Diffie-Hellman key exchange method is not available for all the algorithms. The bit depth for the encryption can be set here.
IPsec SA (Data Exchange)	In contrast to *ISAKMP SA (key exchange)* (see above), the procedure for data exchange is defined here. It does not necessarily have to differ from the procedure defined for key exchange.	
	Algorithms	See above.

IPsec VPN >> Connections >> Edit >> IKE Options		
	Perfect Forward Secrecy (PFS)	Method for providing increased security during data transmission. With IPsec, the keys for data exchange are renewed at defined intervals. With PFS, new random numbers are negotiated with the partner instead of being derived from previously agreed random numbers. The partner must have the same entry. We recommend activation for security reasons. Select **Yes**, if the partner supports PFS. Set *Perfect Forward Secrecy (PFS)* to **No** if the partner is an IPsec/L2TP client.
Lifetimes and Limits	**The keys of an IPsec connection are renewed at defined intervals in order to increase the difficulty of an attack on an IPsec connection.**	
	ISAKMP SA Lifetime	Lifetime in seconds of the keys agreed for ISAKMP SA. Default setting: 3600 seconds (1 hour). The maximum permitted lifetime is 86400 seconds (24 hours).
	IPsec SA Lifetime	Lifetime in seconds of the keys agreed for IPsec SA. Default setting: 28800 seconds (8 hours). The maximum permitted lifetime is 86400 seconds (24 hours).
	IPsec SA Traffic Limit	0 to 2147483647 bytes The value 0 indicates that there is no traffic limit for the IPsec SAs on this VPN connection. All other values indicate the maximum number of bytes which are encrypted by the IPsec SA for this VPN connection (Hard Limit).
	Re-key Margin for Lifetimes	Applies to ISAKMP SAs and IPsec SAs. Minimum duration before the old key expires and during which a new key should be created. Default setting: 540 seconds (9 minutes).

IPsec VPN >> Connections >> Edit >> IKE Options		
	Re-key Margin for the Traffic Limit	Only applies to IPsec SAs. The value 0 indicates that the traffic limit is not used. 0 must be set here when 0 is also set under *IPsec SA Traffic Limit*. If a value above 0 is entered, then a new limit is calculated from two values. The number of bytes entered here is subtracted from the value specified under *IPsec SA Traffic Limit* (i.e., *Hard Limit*). The calculated value is then known as the *Soft Limit*. This specifies the number of bytes which must be encrypted for a new key to be negotiated for the IPsec SA. A further amount is subtracted when a Re-key Fuzz (see below) above 0 is entered. This is a percentage of the re-key margin. The percentage is entered under Re-key Fuzz. The re-key margin value must be lower than the *Hard Limit*. It must be significantly lower when a *Re-key Fuzz* is also added. If the *IPsec SA Lifetime* is reached earlier, the *Soft Limit* is ignored.
	Re-key Fuzz	Maximum percentage by which *Re-key Margin* is to be increased at random. This is used to delay key exchange on machines with multiple VPN connections. Default setting: 100 percent.
	Keying tries	Number of attempts to negotiate new keys with the partner. The value 0 results in unlimited attempts for connections initiated by the mGuard, otherwise it results in 5 attempts.
	Re-key	**Yes/No** When set to **Yes**, the mGuard will attempt to negotiate a new key when the old one expires.
Dead Peer Detection	**If the partner supports the Dead Peer Detection (DPD) protocol, the relevant partners can detect whether or not the IPsec connection is still valid and whether it needs to be established again.**	
	Delay between requests for a sign of life	Duration in seconds after which *DPD Keep Alive* requests should be transmitted. These requests test whether the partner is still available. Default setting: 30 seconds.

IPsec VPN >> Connections >> Edit >> IKE Options		
	Timeout for absent sign of life after which peer is assumed dead	Duration in seconds after which the connection to the partner should be declared dead if there has been no response to the *Keep Alive* requests. Default setting: 120 seconds. If the mGuard finds that a connection is dead, it responds according to the setting under **Connection startup** (see definition of this VPN connection under **Connection startup** on the *General* tab page).

10.3 IPsec VPN >> L2TP over IPsec

These settings are not applied in Stealth mode.

It is not possible to use the MD5 algorithm under Windows 7. The MD5 algorithm must be replaced by SHA-1.

Allows VPN connections to the mGuard to be established using the IPsec/L2TP protocol.

In doing so, the L2TP protocol is driven using an IPsec transport connection in order to establish a tunnel connection to a Point-to-Point Protocol (PPP). Clients are automatically assigned IP addresses by the PPP.

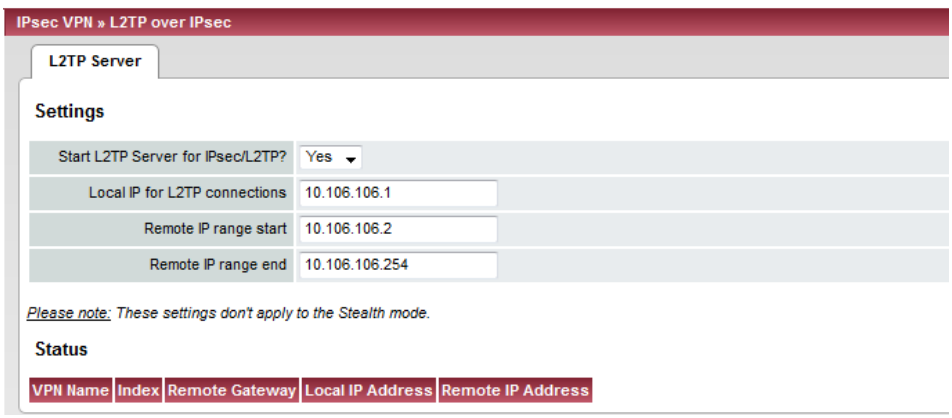
In order to use IPsec/L2TP, the L2TP server must be activated and one or more IPsec connections with the following properties must be defined:

- **Type**: Transport
- **Protocol**: UDP
- **Local:** %all
- **Remote:** %all
- **PFS**: No

See

- IPsec VPN >> Connections >> Edit >> General on Page 257
- IPsec VPN >> Connections >> Edit >> IKE Options, Perfect Forward Secrecy (PFS) on Page 281

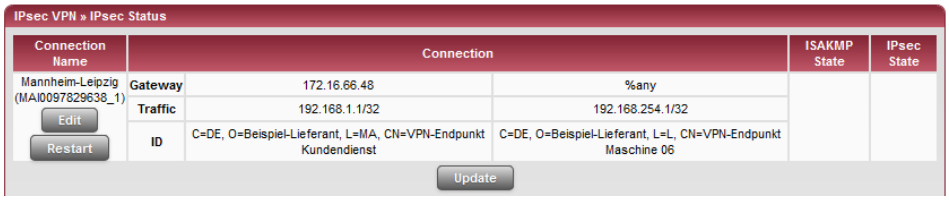
10.3.1 L2TP Server



IPsec VPN >> L2TP over IPsec >> L2TP Server		
Settings	**Start L2TP Server for IPsec/L2TP?**	If you want to enable IPsec/L2TP connections, set this option to **Yes**. It is then possible to establish L2TP connections to the mGuard via IPsec, which dynamically assign IP addresses to the clients within the VPN.
	Local IP for L2TP connections	If set as shown in the screenshot above, the mGuard will inform the partner that its address is 10.106.106.1.

IPsec VPN >> L2TP over IPsec >> L2TP Server		
	Remote IP range start/end	If set as shown in the screenshot above, the mGuard will assign the partner an IP address between 10.106.106.2 and 10.106.106.254.
	Status	Displays information about the L2TP status if this connection type has been selected.

10.4 IPsec VPN >> IPsec Status



Displays information about the status of IPsec connections.

The names of the VPN connections are listed on the left, while their current status is indicated on the right.

Buttons

Update To update the displayed data, if necessary, click on **Update**.

Restart If you want to disconnect and then restart a connection, click on the corresponding **Restart** button.

Edit If you want to reconfigure a connection, click on the corresponding **Edit** button.

Connection, ISAKAMP State, IPsec State

Gateway *Gateway* indicates the IP addresses of the communicating VPN gateways.

Traffic *Traffic* refers to the computers and networks that communicate via the VPN gateways.

ID Refers to the subject of an X.509 certificate.

ISAKMP State *ISAKMP State* (Internet Security Association and Key Management Protocol) is set to “established” if both VPN gateways involved have established a channel for key exchange. In this case, they have been able to contact one another and all entries up to and including “ISAKMP SA” on the connection configuration page are correct.

IPsec State *IPsec State* is set to “established” if IPsec encryption is activated for communication. In this case, the data under “IPsec SA” and “Tunnel Settings” is also correct.

In the event of problems, it is recommended that you check the VPN logs of the partner to which the connection was established. This is because detailed error messages are not forwarded to the initiating computer for security reasons.

If displayed:	This means that:
ISAKMP SA established, IPsec State: WAITING	Authentication was successful, but the other parameters did not match. Does the connection type (tunnel, transport) correspond? If “Tunnel” is selected, do the network areas match on both sides?
IPsec State: IPsec SA established	The VPN connection is established successfully and can be used. However, if this is not possible, the VPN gateway of the partner is causing problems. In this case, deactivate and reactivate the connection to reestablish the connection.

11 SEC-Stick menu

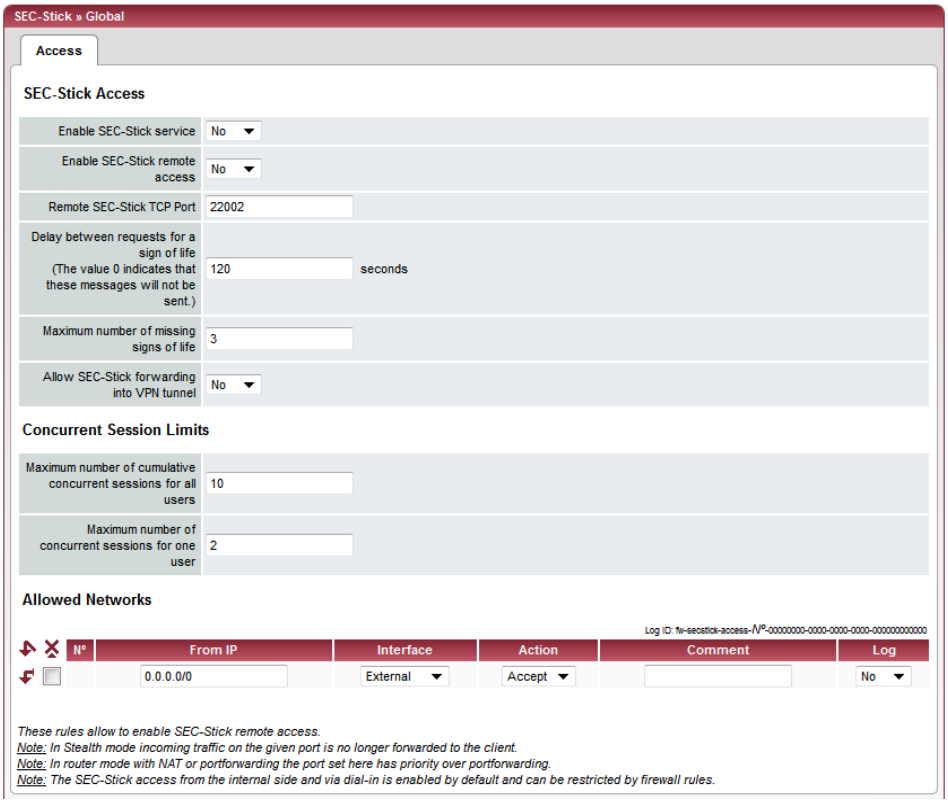
The mGuard supports the use of an SEC-Stick, which is an access protector for IT systems. The SEC-Stick is a product of the team2work company: www.team2work.de

The SEC-Stick is a key. The user inserts it into the USB port of a computer with an Internet connection, and can then set up an encrypted connection to the mGuard in order to securely access defined services in the office or home network. The Remote Desktop Protocol, for example, can be used within the encrypted and secure SEC-Stick connection to control a PC remotely in the office or at home, as if the user was sitting directly in front of it.

In order for this to work, access to the business PC is protected by the mGuard and the mGuard must be configured for the SEC-Stick to permit access because the user of this remote computer, into which the SEC-Stick is inserted, authenticates herself/himself to the mGuard using the data and software stored on her/his SEC-Stick.

The SEC-Stick establishes an SSH connection to the mGuard. Additional channels can be embedded into this connection, e.g., TCP/IP connections.

11.1 Global


SEC-Stick » Global
Access
SEC-Stick Access
Enable SEC-Stick service
No
Enable SEC-Stick remote access
No
Remote SEC-Stick TCP Port
22002
Delay between requests for a sign of life (The value 0 indicates that these messages will not be sent.)
120
seconds
Maximum number of missing signs of life
3
Allow SEC-Stick forwarding into VPN tunnel
No
Concurrent Session Limits
Maximum number of cumulative concurrent sessions for all users
10
Maximum number of concurrent sessions for one user
2
Allowed Networks
N°
From IP
Interface
Action
Comment
Log
0.0.0.0/0
External
Accept
No
These rules allow to enable SEC-Stick remote access.
Note: In Stealth mode incoming traffic on the given port is no longer forwarded to the client.
Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.
Note: The SEC-Stick access from the internal side and via dial-in is enabled by default and can be restricted by firewall rules.

SEC-Stick >> Global >> Access

SEC-Stick Access

This menu item is not included in the scope of functions for the mGuard rs2000 3G, mGuard rs2000.

Access via the SEC-Stick requires a license. This access function can only be used if the corresponding license has been purchased and installed.

Enable SEC-Stick service

Set this option to **Yes** to specify that the SEC-Stick being used at a remote location or its owner is able to log in. In this case, SEC-Stick remote access must also be enabled (next option).

Enable SEC-Stick remote access

Set this option to **Yes** to enable SEC-Stick remote access.

Remote SEC-Stick TCP Port

Default: 22002

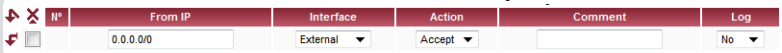
If this port number is changed, the new port number only applies for access via the *External, External 2* or *VPN* interface. Port number 22002 still applies for internal access.

SEC-Stick >> Global >> Access [...]		
	Delay between requests for a sign of life	Default: 120 seconds Values from 0 to 3600 seconds can be set. Positive values indicate that the mGuard is sending a query to the partner within the encrypted SSH connection to find out whether it can still be accessed. The request is sent if no activity was detected from the partner for the specified number of seconds (e.g., due to network traffic within the encrypted connection). The value entered relates to the functionality of the encrypted SSH connection. As long as the functions are working properly, the SSH connection is not terminated by the mGuard as a result of this setting, even when the user does not perform any actions during this time. As the number of simultaneously open sessions is limited (see *Maximum number of cumulative concurrent sessions for all users*), it is important to terminate sessions that have expired. Therefore, the request for a sign of life is preset to 120 seconds in the case of Version 7.4.0 or later. If a maximum of three requests for a sign of life are issued, this causes an expired session to be detected and removed after six minutes. In previous versions, the preset was “0”. This means that no requests for a sign of life are sent. Please note that sign of life requests generate additional traffic.
	Maximum number of missing signs of life	Specifies the maximum number of times a sign of life request to the partner may remain unanswered. For example, if a sign of life request should be made every 15 seconds and this value is set to 3, then the SEC-Stick client connection is deleted if a sign of life is not detected after approximately 45 seconds.
Concurrent session limits	The number of simultaneous sessions is limited for SEC-Stick connections. Approximately 0.5 Mbytes of memory space is required for each session to ensure the maximum level of security. The restriction does not affect existing sessions; it only affects newly established connections.	
	Maximum number of cumulative concurrent sessions for all users	0 to 2147483647 Specifies the number of connections that are permitted for all users simultaneously. When “0” is set, no session is permitted.
	Maximum number of concurrent sessions for one user	0 to 2147483647 Specifies the number of connections that are permitted for one user simultaneously. When “0” is set, no session is permitted.

SEC-Stick >> Global >> Access [...]

Allowed Networks

Lists the firewall rules that have been set up for SEC-Stick remote access.



If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

The rules specified here only take effect if **Enable SEC-Stick remote access** is set to **Yes**. *Internal* access is also possible when this option is set to *No*. A firewall rule that would refuse *Internal* access does therefore not apply in this case.

Multiple rules can be specified.

From IP

Enter the address of the computer/network from which remote access is permitted or forbidden in this field.

IP address **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).

Interface

External/Internal/External 2/VPN/Dial-in[1]

Specifies to which interface the rule should apply.

If no rules are set or if no rule applies, the following default settings apply:

– Remote SEC-Stick access is permitted via *Internal, VPN*, and *Dial-in*.

– Access via *External* and *External 2* is refused.

Specify the access options according to your requirements.

If you want to refuse access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as an action.

Action

Accept means that the data packets may pass through.

Reject means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.)

Drop means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.

Comment

Freely selectable comment for this rule.

Log

For each individual firewall rule, you can specify whether the use of the rule:

– Should be logged – set *Log* to **Yes**

– Should not be logged – set *Log* to **No** (default setting)

1 *External 2* and *Dial-in* are only for devices with a serial interface (see “Network >> Interfaces” on page 105).

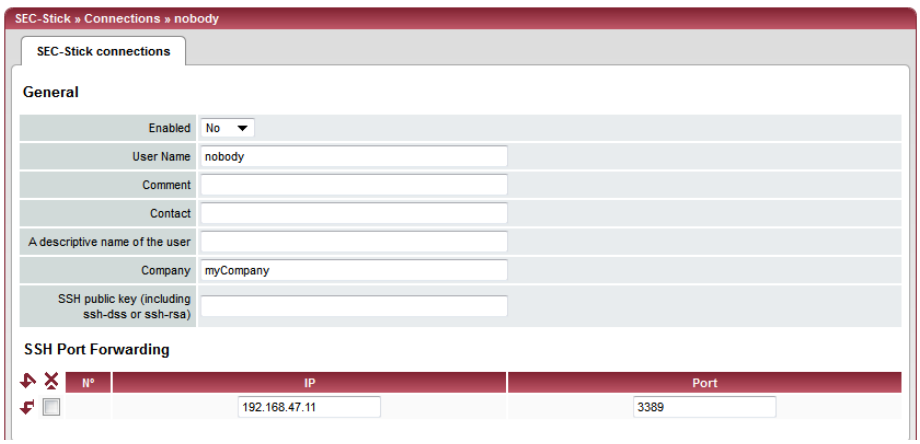
11.2 Connections

SEC-Stick >> Connections >> SEC-Stick connections	
SEC-Stick connections	**List of defined SEC-Stick connections. Click on the down arrow at the top left of the screen if you want to add a new connection. An existing connection can be edited by clicking on Edit.**

Not all of the SEC-Stick functions can be configured via the web interface of the mGuard.

Enabled	To use a defined SEC-Stick connection, the **Enabled** option must be set to **Yes**.
User Name	An SEC-Stick connection with a uniquely assigned user name must be defined for every owner of a SEC-Stick who has authorized access. This user name is used to uniquely identify the defined connections.
Name	Name of the person.
Company	Name of the company.

The following page appears when you click on **Edit**:



General	**Enabled**	As above
	User Name	As above
	Comment	Optional comment text.
	Contact	Optional comment text.
	A descriptive name of the user	Optional name of the person (repeated).

SEC-Stick >> Connections >> SEC-Stick connections [...]		
	Company	Optional: As above
	SSH public key (including ssh-dss or ssh-rsa)	Enter the SSH public key belonging to the SEC-Stick in ASCII format in this field. The secret equivalent is stored on the SEC-Stick.
SSH Port Forwarding	**List of allowed access and SSH port forwarding relating to the SEC-Stick of the corresponding user.**	
	IP	IP address of the computer to which access is enabled.
	Port	Port number to be used when accessing the computer.

12 QoS menu

This menu is **not** available on the **mGuard rs2000 (3G)**.

QoS (Quality of Service) refers to the quality of individual transmission channels in IP networks. This relates to the allocation of specific resources to specific services or communication types so that they work correctly. The necessary bandwidth, for example, must be provided to transmit audio or video data in realtime in order to reach a satisfactory communication level. At the same time, slower data transfer by FTP or e-mail does not threaten the overall success of the transmission process (file or e-mail transfer).

12.1 Ingress Filters

An ingress filter prevents the processing of certain data packets by filtering and dropping them before they enter the mGuard processing mechanism. The mGuard can use an ingress filter to avoid processing data packets that are not needed in the network. This results in a faster processing of the remaining, i.e., required data packets.

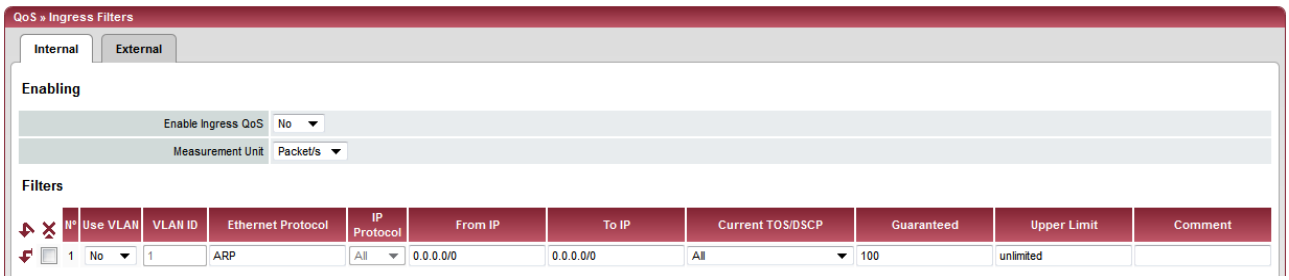
Using suitable filter rules, administrative access to the mGuard can be ensured with high probability, for example.

Packet processing on the mGuard is generally defined by the handling of individual data packets. This means that the processing performance depends on the number of packets to be processed and not on the bandwidth.

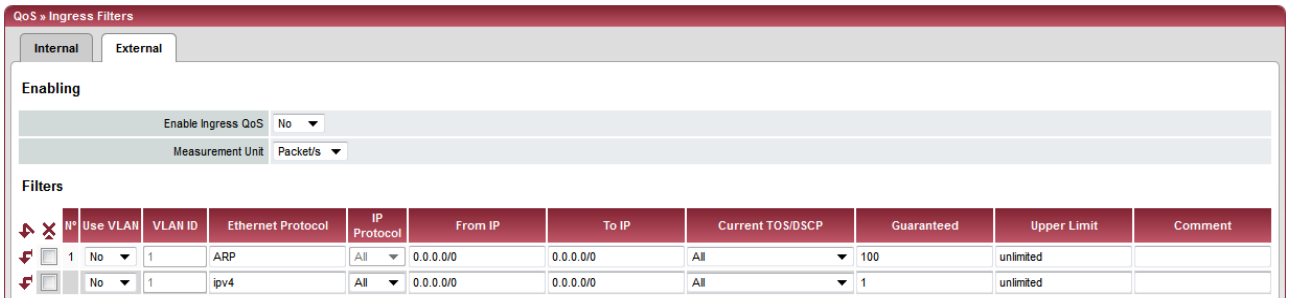
Filtering is performed exclusively according to features that are present or may be present in each data packet: the sender and recipient IP address specified in the header, the specified Ethernet protocol, the specified IP protocol, the specified TOS/DSCP value, and/or the VLAN ID (if VLANs have been set up). As the list of filter rules must be applied to each individual data packet, it should be kept as short as possible. Otherwise, the time spent on filtering could be longer than the time actually saved by setting the filter.

Please note that not all specified filter criteria should be combined. For example, it does not make sense to specify an additional IP protocol in the same rule that contains the ARP Ethernet protocol. Nor does it make sense to specify a transmitter or sender IP address if the IPX Ethernet protocol is specified (in hexadecimal format).

12.1.1 Internal/External



Internal: settings for the ingress filter at the LAN interface



External: settings for the ingress filter at the WAN interface

QoS >> Ingress Filters >> Internal/External		
Enabling	**Enable Ingress QoS**	**No** (default): this feature is disabled. If filter rules are defined, they are ignored. **Yes**: this feature is enabled. Data packets may only pass through and be forwarded to the mGuard for further evaluation and processing if they comply with the filter rules defined below. Filters can be set for the LAN port (**Internal** tab page) and the WAN port (**External** tab page).
	Measurement Unit	**kbps or Packet/s** Specifies the unit of measurement for the numerical values entered under **Guaranteed** and **Upper Limit**.
Filter	**Use VLAN**	If a VLAN is set up, the relevant VLAN ID can be specified to allow the relevant data packets to pass through. To do this, this option must be set to **Yes**.
	VLAN ID	Specifies that the VLAN data packets that have this VLAN ID may pass through. (To do this, the **Use VLAN** option must be set to **Yes**.)
	Ethernet Protocol	Specifies that only data packets of the specified Ethernet protocol may pass through. Possible entries: **ARP**, **IPV4**, **%any**. Other entries must be in hexadecimal format (up to 4 digits). (The ID of the relevant protocol in the Ethernet header is entered here. It can be found in the publication of the relevant standard.)
	IP Protocol	**All/TCP/UDP/ICMP/ESP** Specifies that only data packets of the selected IP protocol may pass through. When set to **All**, no filtering is applied according to the IP protocol.
	From IP	Specifies that only data packets from a specified IP address may pass through. **0.0.0.0/0** stands for all addresses, i.e., in this case no filtering is applied according to the IP address of the sender. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24).

QoS >> Ingress Filters >> Internal/External[...]		
	To IP	Specifies that only data packets that should be forwarded to the specified IP address may pass through. Entries correspond to *From IP*, as described above. **0.0.0.0/0** stands for all addresses, i.e., in this case no filtering is applied according to the IP address of the sender.
	Current TOS/DSCP	Each data packet contains a TOS or DSCP field. (TOS stands for Type of Service, DSCP stands for Differentiated Services Code Point). The traffic type to which the data packet belongs is specified here. For example, an IP phone will write a different entry in this field for outgoing data packets compared to an FTP program. When a value is selected here, only data packets with this value in the TOS or DSCP field may pass through. When set to **All**, no filtering according to the TOS/DSCP value is applied.
	Guaranteed	The number entered specifies how many data packets per second or kbps can pass through at all times – according to the option set under **Measurement Unit** (see above). This applies to the data stream that conforms to the rule set criteria specified on the left (i.e., that may pass through). The mGuard **may** drop the excess number of data packets in the event of capacity bottlenecks if this data stream delivers more data packets per second than specified.
	Upper Limit	The number entered specifies the maximum number of data packets per second or kbps that can pass through – according to the option set under **Measurement Unit** (see above). This applies to the data stream that conforms to the rule set criteria specified on the left (i.e., that may pass through). The mGuard drops the excess number of data packets if this data stream delivers more data packets per second than specified.
	Comment	Optional comment text.

12.2 Egress Queues

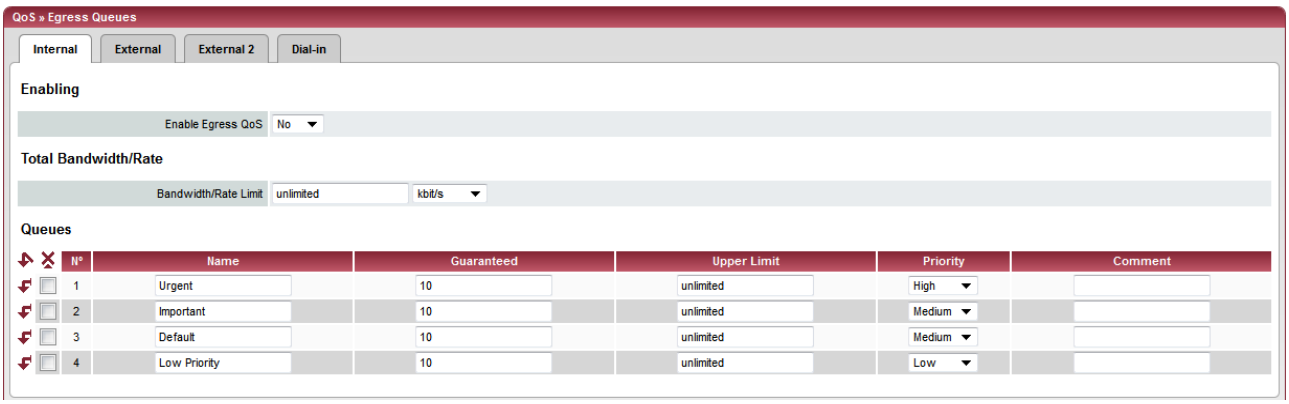
The services are assigned corresponding priority levels. In the event of connection bottlenecks, the outgoing data packets are placed in egress queues (i.e., queues for pending packets) according to the assigned priority level and are then processed according to their priority. Ideally, the assignment of priority levels and bandwidths should result in a sufficient bandwidth level always being available for the realtime transmission of data packets, while other packets, e.g., FTP downloads, are temporarily set to wait in critical cases.

The main application of egress QoS is the optimal utilization of the available bandwidth on a connection. In certain cases, a limitation of the packet rate can be useful, e.g., to protect a slow computer from overloading in the protected network.

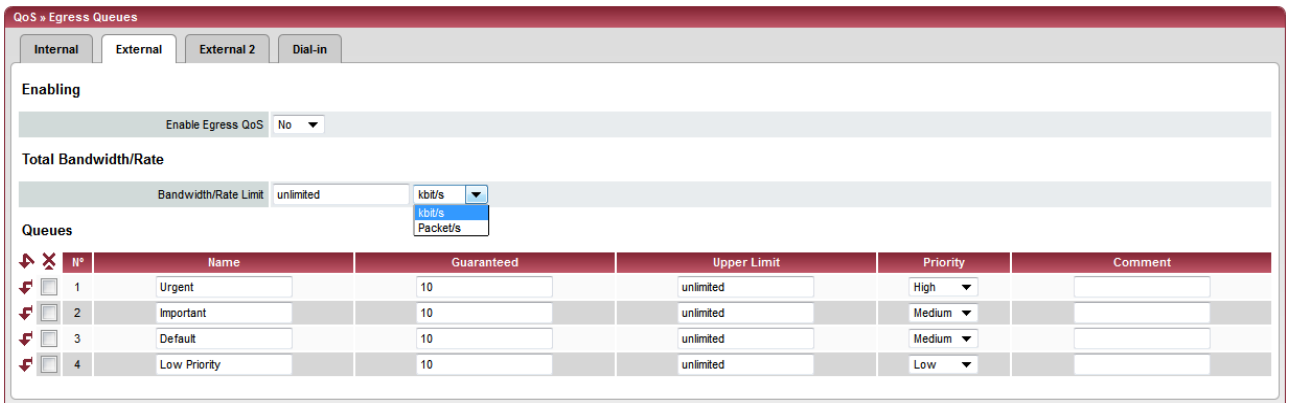
The *Egress Queues* feature can be used for all interfaces and for VPN connections.

12.2.1 Internal/External/External 2/Dial-in

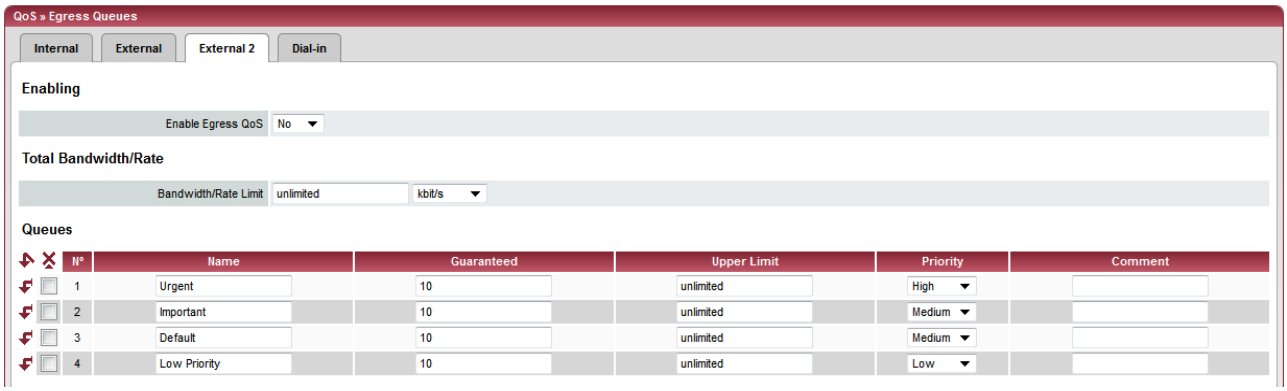
Internal: settings for egress queues on the LAN interface



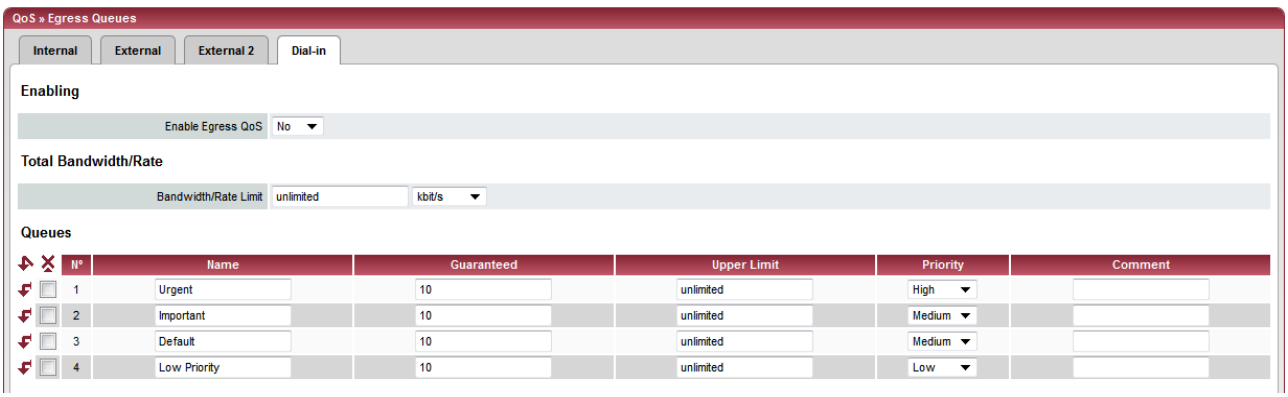
External: settings for egress queues on the external WAN interface



External 2: settings for egress queues on the secondary external interface



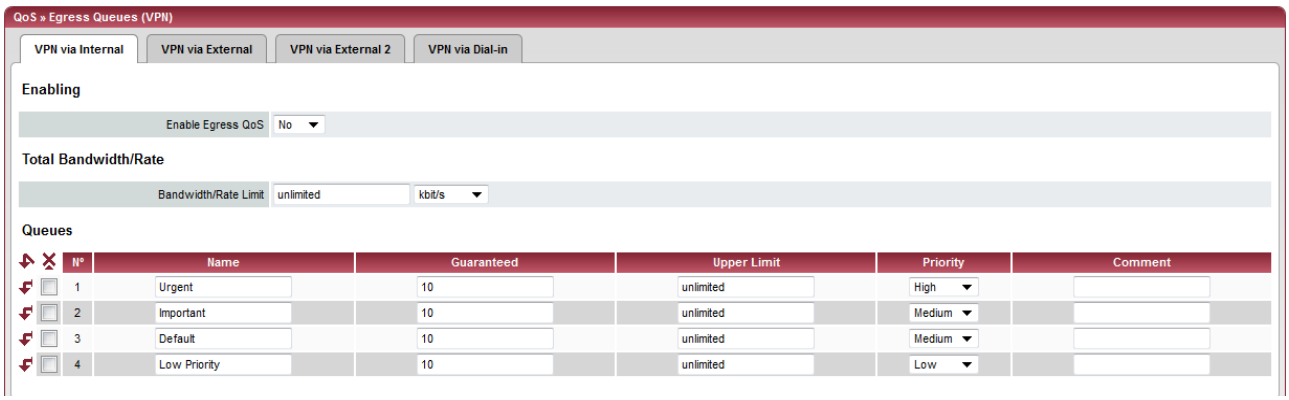
Dial-in: settings for egress queues for packets for a PPP dial-up connection (dial-in)



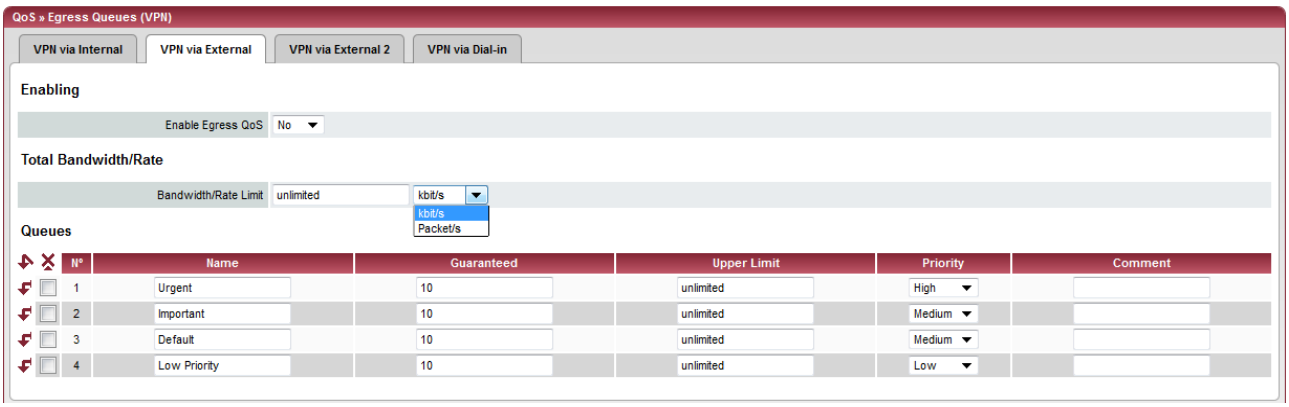
12.3 Egress Queues (VPN)

12.3.1 VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in

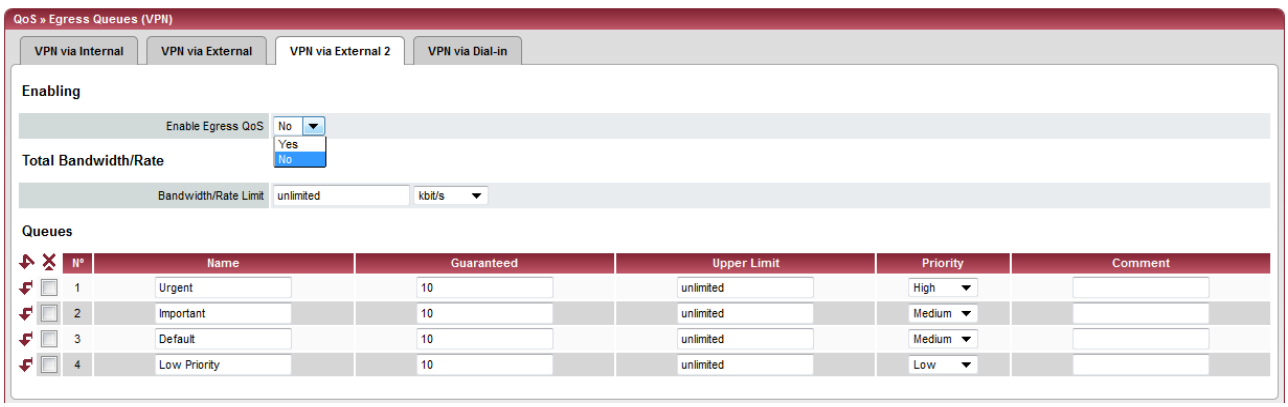
VPN via Internal: settings for egress queues



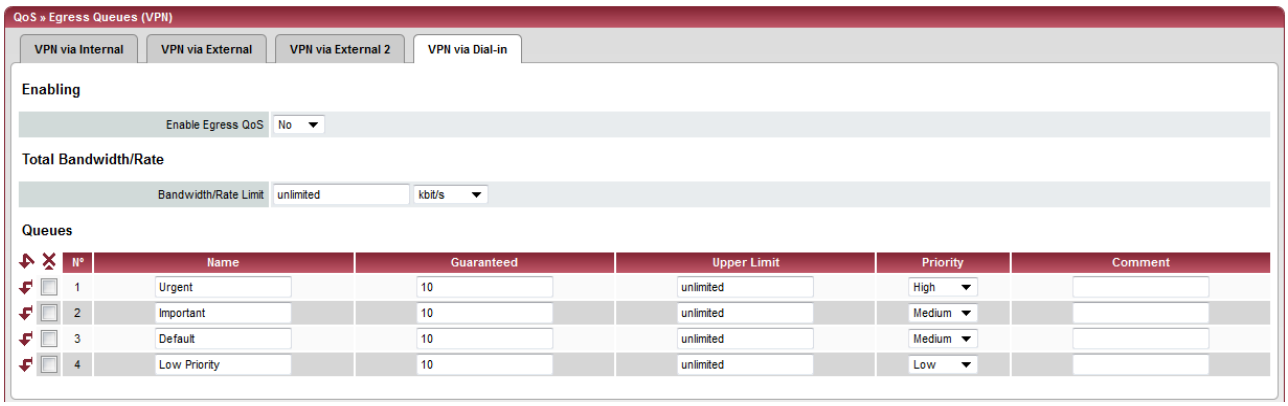
VPN via External: settings for egress queues



VPN via External 2: settings for egress queues



VPN via Dial-in: settings for egress queues



All of the tab pages listed above for *Egress Queues* for the *Internal, External, External 2,* and *Dial-in* interfaces, and for VPN connections routed via these interfaces, have the same setting options.

In all cases, the settings relate to the data that is sent externally into the network from the relevant mGuard interface.

QoS menu >> Egress Queues >> Internal/External/External 2/Dial-in

QoS menu >> Egress Queues (VPN) >> VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in

Enabling	**Enable Egress QoS**	**No** (default): this feature is disabled. **Yes**: this feature is enabled. This option is recommended if the interface is connected to a network with low bandwidth. This enables bandwidth allocation to be influenced in favor of particularly important data.
Total Bandwidth/Rate	**Bandwidth/Rate Limit**	**kbps or Packet/s** Total maximum bandwidth that is physically available – specified in kbps or packets per second. In order to optimize prioritization, the total bandwidth specified here should be slightly lower than the actual amount. This prevents a buffer overrun on the transferring devices, which would result in adverse effects.
Queues	**Name**	The default name for the egress queue can be adopted or another can be assigned. The name does not specify the priority level.
	Guaranteed	Bandwidth that should be available at all times for the relevant queue. Based on the selection under **Bandwidth/Rate Limit** (**kbps** OR **Packet/s**), meaning that the unit of measurement does not have to be specified explicitly here. The total of all guaranteed bandwidths must be less than or equal to the total bandwidth.

QoS menu >> Egress Queues >> Internal/External/External 2/Dial-in QoS menu >> Egress Queues (VPN) >> VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in[...]		
	Upper Limit	Maximum bandwidth available that may be set for the relevant queue by the system. Based on the selection under **Bandwidth/Rate Limit** (**kbps** OR **Packet/s**), meaning that the unit of measurement does not have to be specified explicitly here. The value must be greater than or equal to the guaranteed bandwidth. The value **unlimited** can also be specified, which means that there is no further restriction.
	Priority	**Low/Medium/High** Specifies with which priority the affected queue should be processed, provided the total available bandwidth has not been exhausted.
	Comment	Optional comment text.

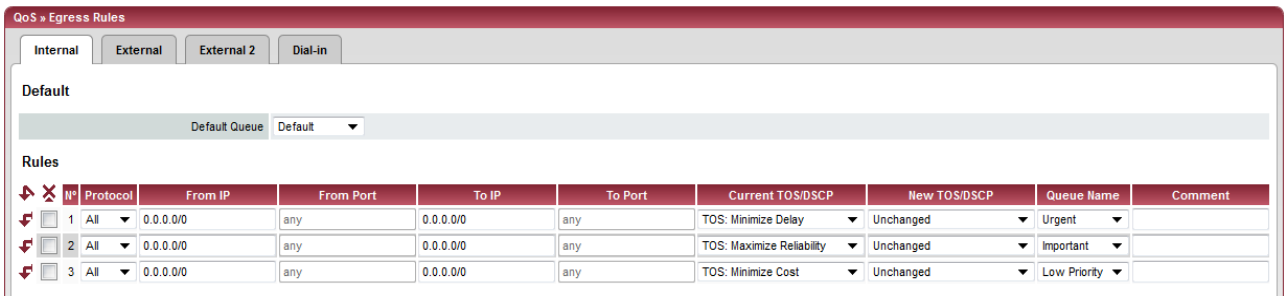
12.4 Egress Rules

This page defines the rules for the data that is assigned to the defined egress queues (see above) in order for the data to be transmitted with the priority assigned to the relevant queue.

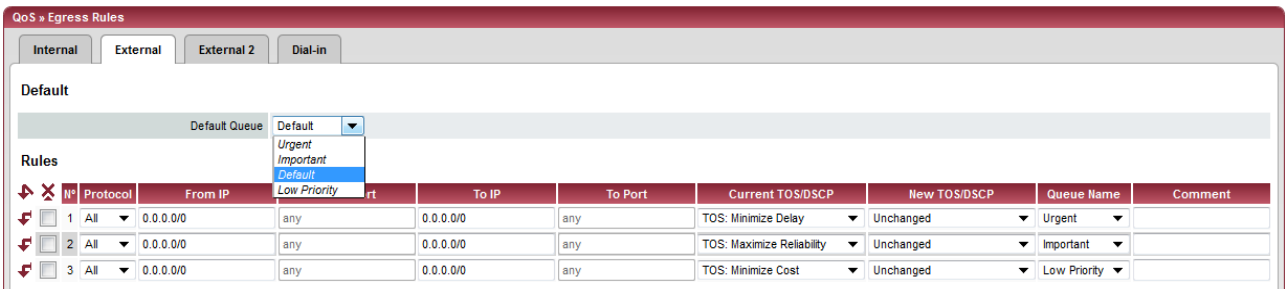
Rules can be defined separately for all interfaces and for VPN connections.

12.4.1 Internal/External/External 2/Dial-in

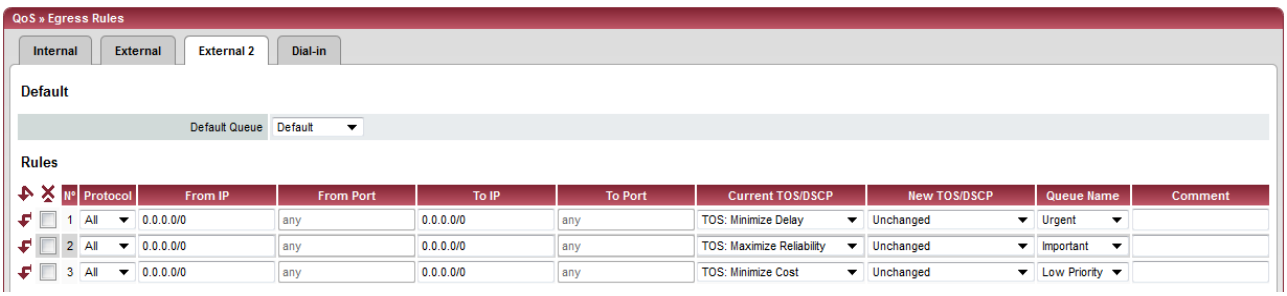
Internal: settings for egress queue rules



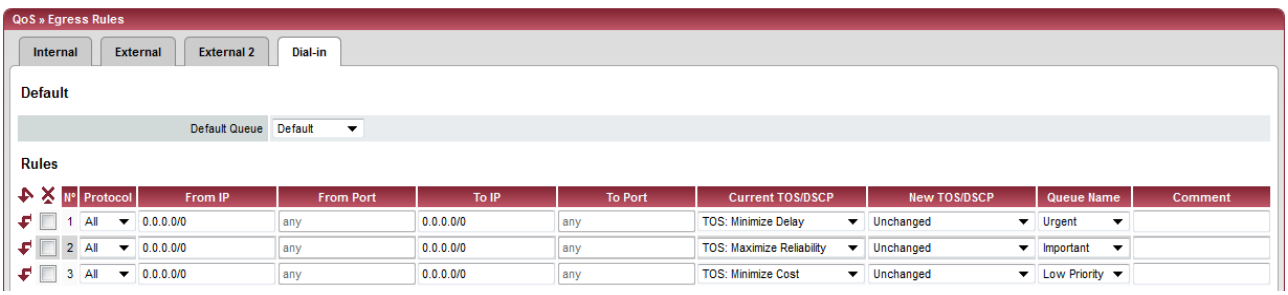
External: settings for egress queue rules



External 2: settings for egress queue rules



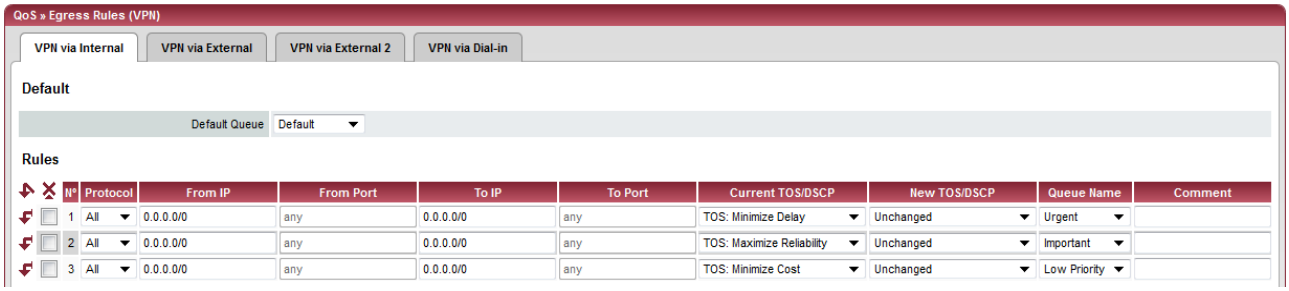
Dial-in: settings for egress queue rules



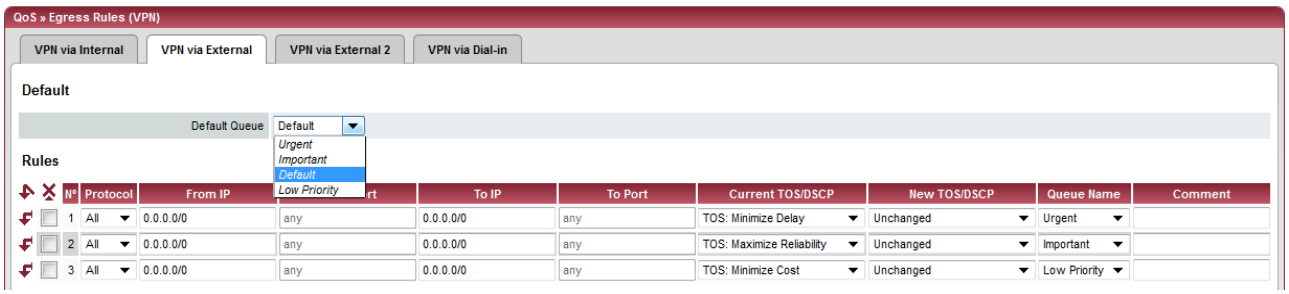
12.4.2 Egress Rules (VPN)

VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in

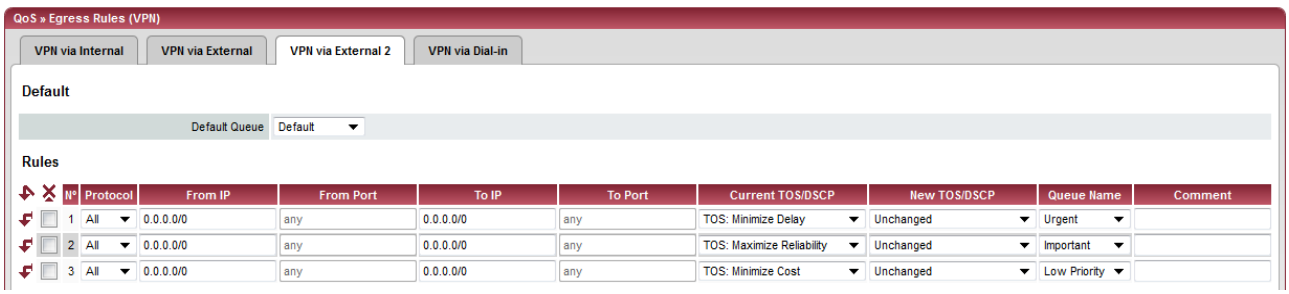
VPN via Internal: settings for egress queue rules



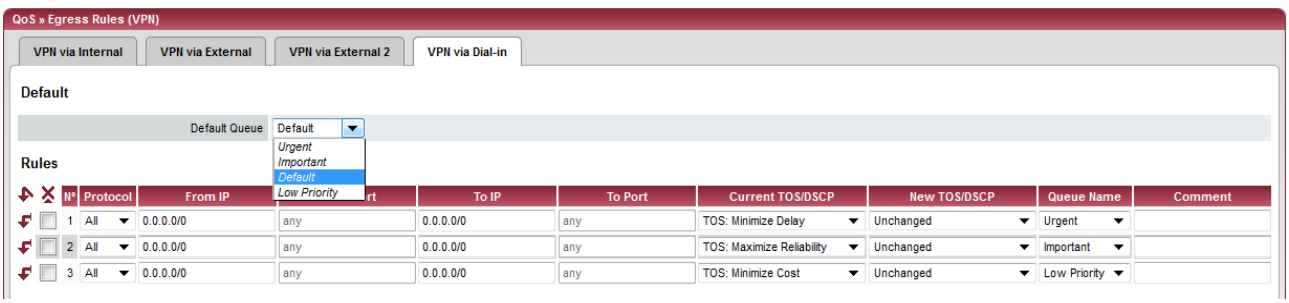
VPN via External: settings for egress queue rules



VPN via External 2: settings for egress queue rules



VPN via Dial-in: settings for egress queue rules



All of the tab pages listed above for *Egress Rules* for the *Internal, External, External 2,* and *Dial-in* interfaces, and for VPN connections routed via these interfaces, have the same setting options.

In all cases, the settings relate to the data that is sent externally into the network from the relevant mGuard interface.

QoS menu >> Egress Rules >> Internal/External/External 2/Dial-in QoS menu >> Egress Rules (VPN) >> VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in		
Default	**Default Queue**	*Name of the egress queue* (user-defined). The names of the queues are displayed as listed or specified under *Egress Queues* on the *Internal*/*External*/*VPN via External* tab pages. The following default names are defined: Default/Urgent/Important/Low Priority. Traffic that is **not** assigned to a specific egress queue under *Rules* remains in the *default queue*. You can specify which egress queue should be used as the *default queue* in this selection list.
	Rules	The assignment of specific data traffic to an egress queue is based on a list of criteria. If the criteria in a row apply to a data packet, it is assigned to the egress queue specified in the row. **Example**: for audio data to be transmitted, you have defined a queue with guaranteed bandwidth and priority under Egress Queues (see Page 296) under the name *Urgent*. You then define the rules here for how audio data is detected and specify that this data should belong to the *Urgent* queue.
	Protocol	**All/TCP/UDP/ICMP/ESP** Protocol(s) relating to the rule.
	From IP	IP address of the network or device from which the data originates. **0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 24). Assign the traffic from this source to the queue selected under *Queue Name* in this row.
	From Port	Port used at the source from which data originates (only evaluated for TCP and UDP protocols). – **any** refers to any port. – **startport:endport** (e.g., 110:120) refers to a port area. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
	To IP	IP address of the network or device to which the data is sent. Entries correspond to *From IP*, as described above.
	To Port	Port used at the source where the data is sent. Entries correspond to *From Port*, as described above.

QoS menu >> Egress Rules >> Internal/External/External 2/Dial-in

QoS menu >> Egress Rules (VPN) >> VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in [...]

Current TOS/DSCP	Each data packet contains a TOS or DSCP field. (TOS stands for Type of Service, DSCP stands for Differentiated Services Code Point). The traffic type to which the data packet belongs is specified here. For example, an IP phone will write a different entry in this field for outgoing data packets compared to an FTP program that uploads data packet to a server. When you select a value here, only the data packets that have this TOS or DSCP value in the corresponding fields are chosen. These values are then set to a different value according to the entry in the **New TOS/DSCP** field.
New TOS/DSCP	If you want to change the TOS/DSCP values of the data packets that are selected using the defined rules, enter the text that should be written in the TOS/DSCP field here. For a more detailed explanation of the **Current TOS/DSCP** and **New TOS/DSCP** options, please refer to the following RFC documents: – RFC 3260 “New Terminology and Clarifications for Diffserv” – RFC 3168 “The Addition of Explicit Congestion Notification (ECN) to IP” – RFC 2474 “Definition of the Differentiated Services Field (DS Field)” – RFC 1349 “Type of Service in the Internet Protocol Suite”
Queue Name	Name of the egress queue to which traffic should be assigned.
Comment	Optional comment text.

13 Redundancy menu

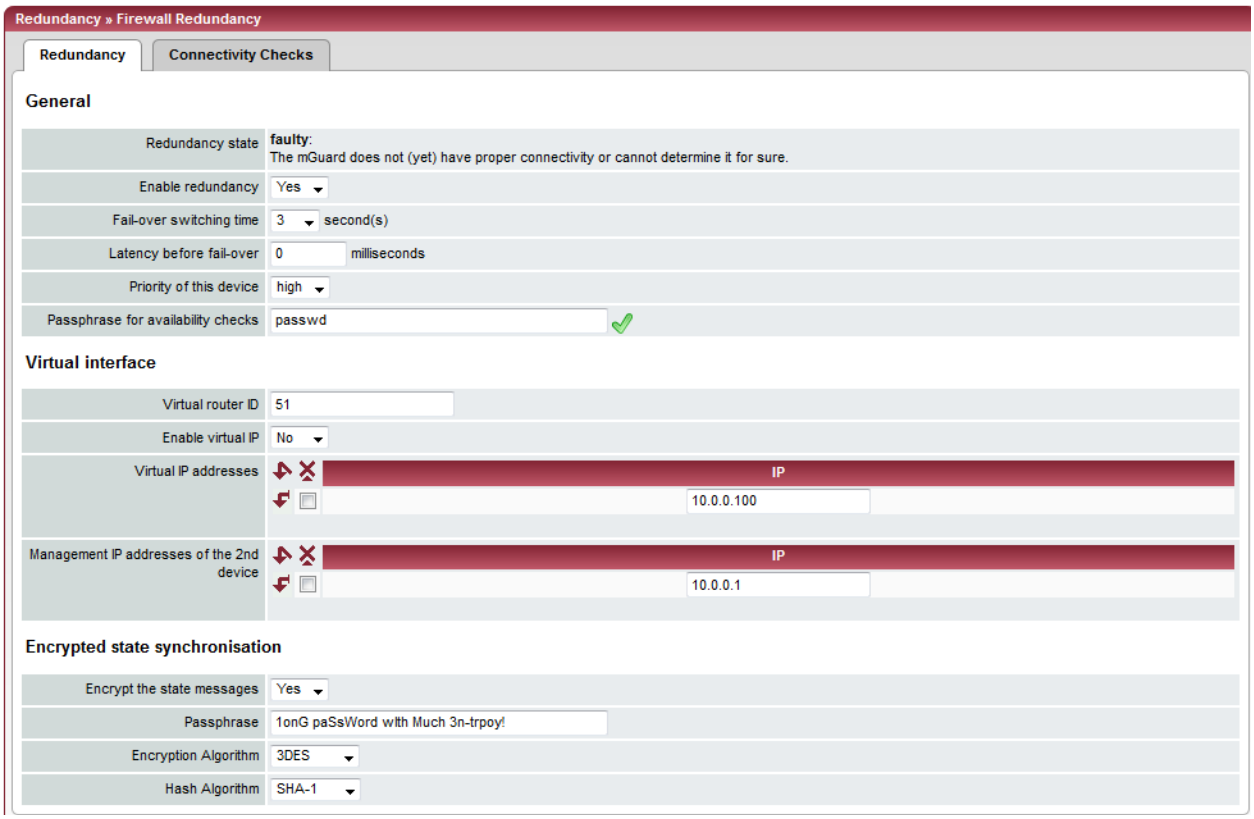
Redundancy is described in detail in Section 16, “Redundancy”.

To use the redundancy function, both mGuards must have the same firmware.

13.1 Redundancy >> Firewall Redundancy

This menu is **not** available on the **mGuard rs2000** and **mGuard rs2000 3G**.

13.1.1 Redundancy



Redundancy >> Firewall Redundancy >> Redundancy		
General	**Redundancy state**	Shows the current status.
	Enable redundancy	**No** (default): firewall redundancy is disabled. **Yes**: firewall redundancy is enabled. This function can only be activated when a suitable license key is installed. Further conditions apply if VPN redundancy is to be enabled at the same time, see “VPN redundancy” on page 345.
	Fail-over switching time	Maximum time that is allowed to elapse in the event of errors before switching to the other mGuard.
	Waiting time prior to switching	**0 ... 10000 milliseconds, default: 0** Time the redundancy system ignores an error. The connectivity and availability checks ignore an error until it is still present after the time set here has elapsed.
	Priority of this device	**high/low** Specifies the priority associated with the presence notifications (CARP). Set the priority to **high** on the mGuard that you want to be active. The mGuard on standby is set to **low**. Both mGuard devices in a redundant pair may either be set to different priorities or be assigned the **high** priority. Never set **both** mGuard devices in a redundant pair to **low** priority.

Redundancy >> Firewall Redundancy >> Redundancy

Passphrase for availability checks

On an mGuard which is part of a redundant pair, checks are constantly performed to determine whether an active mGuard is available and whether it should remain active. A variation of the CARP (Common Address Redundancy Protocol) is used here.

CARP uses SHA-1 HMAC encryption together with a password. This password must be set so it is the same for both mGuard devices. It is used for encryption and is never transmitted in plain text.

The password is important for security since the mGuard is vulnerable at this point. We recommend a password with at least 20 characters and numerous special characters (printable UTF-8 characters). It must be changed on a regular basis.

When changing the password, proceed as follows:

Check the status of the set password before you enter a new one.

There is only a valid password available and you are only permitted to enter a new password if you can see a **green check mark** to the right of the entry field.

Set the new password on both mGuard devices. It does not matter which order you do this in but the same password must be used in both cases. If you inadvertently enter an incorrect password, follow the instructions under “How to proceed in the event of an incorrect password” on page 308.

As soon as a redundant pair has been assigned a new password, it automatically negotiates when it can switch to the new password without interruption.

The status is displayed using symbols. We recommend observing this status for security reasons.

A **red cross** indicates that the mGuard has a new password that it wants to use. However, the old password is still in use.

A **yellow check mark** indicates that the new password is already in use but that the old password can still be accepted in case the other mGuard still uses it.

If **no symbol** is shown, it means that no password is being used. For example, this may be because redundancy has not been activated or the firmware is booting up.

If an mGuard fails while the password is being changed, the following scenarios apply:

– Password replacement has been started on all mGuard devices and then interrupted because of a network error, for example. This scenario is rectified automatically.

– Password replacement has been started on all mGuard devices. However, an mGuard then fails and must be replaced.

  Examine the remaining mGuard to determine whether the process of changing the password has been completed. If you can see a green check mark, you must set the new password directly on the mGuard that is being replaced.

  If you cannot see a green check mark, it means that the password has not yet been changed on the remaining mGuard. In this case, you must change the password again on the mGuard that is still in operation. Wait until the green check mark appears. Only then should you replace the mGuard that has failed. Configure the replacement mGuard with the new password immediately on setting up redundancy.

– Password replacement has been started but not performed on all mGuard devices because they have failed. Password replacement must be started as soon as a faulty mGuard is back online. If an mGuard has been replaced, it must first be configured with the old password before it is connected.

How to proceed in the event of an incorrect password

If you have inadvertently entered an incorrect password on an mGuard, proceed as follows.

If you can still remember the old password, proceed as follows:

- Reconfigure the mGuard on which the incorrect password was entered so that it uses the old password.
- Wait until the mGuard indicates that the old password is being used.
- Then enter the correct password.

If you have forgotten the old password, proceed as follows:

- Check whether you can read the old password out from the other mGuard.
- If the other mGuard is disabled or missing, you can simply enter the correct new password on the active mGuard on which you inadvertently set the incorrect password. Make sure that the other mGuard is assigned the same password before operating it again.
- If the other mGuard is already using the new password, you must make sure that the mGuard with the incorrect password is not active or able to be activated, e.g., by removing the cable at the LAN or WAN interface.

  In the case of remote access, you can enter a destination for the connectivity check that will not respond. Prior to provoking this kind of error, check that there is no redundancy error on any of the mGuard devices. One mGuard must be active and the other must be on standby. It might be necessary to rectify any errors displayed and only then use this method. After that, follow these steps:
  – Replace the incorrect password with a different one.
  – Enter this password on the active mGuard too.
  – Restart the mGuard that is not active. You can do this, for example, by reconnecting the Ethernet cable or restoring the old settings for the connectivity check.

Redundancy >> Firewall Redundancy >> Redundancy		
Virtual interfaces	**External virtual Router ID**	**1, 2, 3, ... 255 (default: 51)** Only in Router network mode. This ID is sent by the redundant pair with each presence notification (CARP) via the external interface and is used to identify the redundant pair. This ID must be the same for both mGuard devices. It is used to differentiate the redundant pair from other redundant pairs that are connected to the same Ethernet segment through their external interface. Please note that CARP uses the same protocol and port as VRRR (Virtual Router Redundancy Protocol). The ID set here must be different to the IDs on other devices which use VRRR or CARP and are located in the same Ethernet segment.
	External virtual IP addresses	Default: 10.0.0.100 Only in Router network mode. These are IP addresses which are shared by both mGuard devices as virtual IP addresses of the external interface. These IP addresses must be the same for both mGuard devices. These addresses are used as a gateway for explicit static routes for devices located in the same Ethernet segment as the external network interface of the mGuard. The active mGuard can receive ICMP queries via this IP address. It reacts to these ICMP requests depending on the menu settings under *Network Security >> Packet Filter >> Advanced*. No subnet masks or VLAN IDs are set up for the virtual IP addresses as these attributes are defined by the actual external IP address. For each virtual IP address, an actual IP address must be configured whose IP network accommodates the virtual address. The mGuard transmits the subnet mask and VLAN setting from the actual external IP address to the corresponding virtual IP address. The applied VLAN settings define whether standard MTU settings or VLAN MTU settings are used for the virtual IP address. Firewall redundancy cannot function correctly if no actual IP address and subnet mask are available.

Redundancy >> Firewall Redundancy >> Redundancy		
	Internal virtual Router ID	**1, 2, 3, ... 255 (default: 51)** Only in Router network mode. This ID is sent by the redundant pair with each presence notification (CARP) via the external and internal interface and is used to identify the redundant pair. This ID must be set so it is the same for both mGuard devices. It is used to differentiate the redundant pair from other Ethernet devices that are connected to the same Ethernet segment through their external/internal interface. Please note that CARP uses the same protocol and port as VRRR (Virtual Router Redundancy Protocol). The ID set here must be different to the IDs on other devices which use VRRR or CARP and are located in the same Ethernet segment.
	Internal virtual IP addresses	As described under *External virtual IP addresses*, but with two exceptions. Under **Internal virtual IP addresses**, IP addresses are defined for devices which belong to the internal Ethernet segment. These devices must use the IP address as their default gateway. These addresses can be used as a DNS or NTP server when the mGuard is configured as a server for the protocols. For each virtual IP address, an actual IP address must be configured whose IP network accommodates the virtual address. The response to ICMP requests with internal virtual IP addresses is independent from the settings made under *Network Security >> Packet Filter >> Advanced.*
Encrypted state synchronisation	**Encrypt the state messages**	**Yes/No** If **Yes** is selected, state synchronization is encrypted.
	Passphrase	The password is changed as described under “Passphrase for availability checks” on page 307. Only deviate from the prescribed approach if an incorrect password has been inadvertently entered.

Redundancy >> Firewall Redundancy >> Redundancy

How to proceed in the event of an incorrect password

If you have inadvertently entered an incorrect password on an mGuard, you cannot simply reenter the password using the correct one. Otherwise, in the event of adverse circumstances, this may result in both mGuard devices being active.

Case 1: only one mGuard has an incorrect password. The process of changing the password has not yet begun on the other mGuard.

- Reconfigure the mGuard on which the incorrect password was entered so that it uses the old password.
- Wait until the mGuard indicates that the old password is being used.
- Then enter the correct password.

Case 2: the other mGuard is already using the new password.

- The status of both mGuard devices must be such that they are using an old password but expecting a new one (red cross). To ensure that this is the case, enter random passwords successively.
- Finally, generate a secure password and enter it on both mGuard devices. This password is used immediately without any coordination.

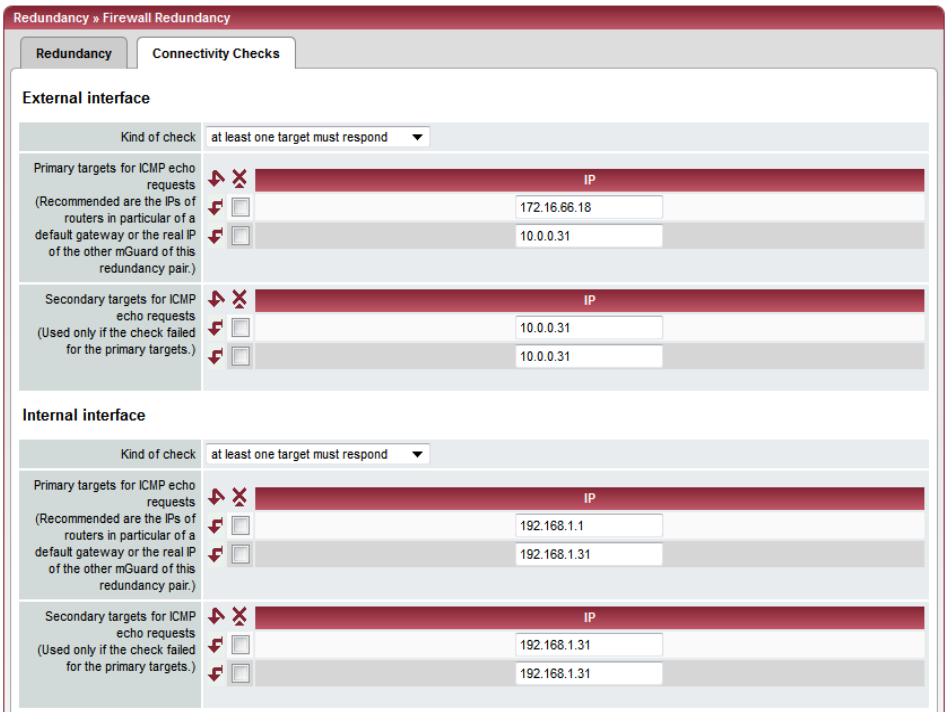
During this process, the state of the mGuard on standby may briefly switch to “outdated”. However, this situation resolves itself automatically.

	Encryption Algorithm	**DES, 3DES, AES-128, AES-192, AES-256** See “Algorithms” on page 280.
	Hash Algorithm	**MD5, SH1, SHA-256, SHA-512** See “Algorithms” on page 280.
Interface for state synchronisation	**Interface which is used for state synchronization**	**Internal Interface/Dedicated Interface** The *mGuard centerport* supports a **dedicated interface**. This is a reserved, direct Ethernet interface or a dedicated LAN segment, via which the state synchronization is sent. The redundant pair can be connected through an additional dedicated Ethernet interface or an interconnected switch. On a **Dedicated Interface**, presence notifications (CARP) are also listened for on the third Ethernet interface. Presence notifications (CARP) are also transmitted when the mGuard is active. However, no additional routing is supported for this interface. Frames received on this interface are not forwarded for security reasons. The connection status of the third Ethernet interface can be queried via SNMP.

Redundancy >> Firewall Redundancy >> Redundancy		
	IP of the dedicated interface	Only available when **Dedicated Interface** is selected. **IP** IP address used on the third network interface of the *mGuard centerport* for state synchronization with the other mGuard. Default: 192.168.68.29 **Netmask** Subnet mask used on the third network interface of the *mGuard centerport* for state synchronization with the other mGuard. Default: 255.255.255.0 **Use VLAN** When **Yes** is selected, a VLAN ID is used for the third network interface. **VLAN ID** 1, 2, 3, ... 4094 (default: 1) VLAN ID when this setting is activated.
	Disable the availability check at the external interface	Only available when **Dedicated Interface** is selected. When **Yes** is selected, no presence notifications (CARP) are transmitted or received via the external interface. This can make sense in some scenarios for protection against external attacks.

13.1.2 Connectivity Checks

Targets can be configured for the internal and external interface in the connectivity check. It is important that these targets are actually connected to the specified interface. An ICMP echo reply cannot be received by an external interface when the corresponding target is connected to the internal interface (and vice versa). When the static routes are changed, the targets may easily not be checked properly.

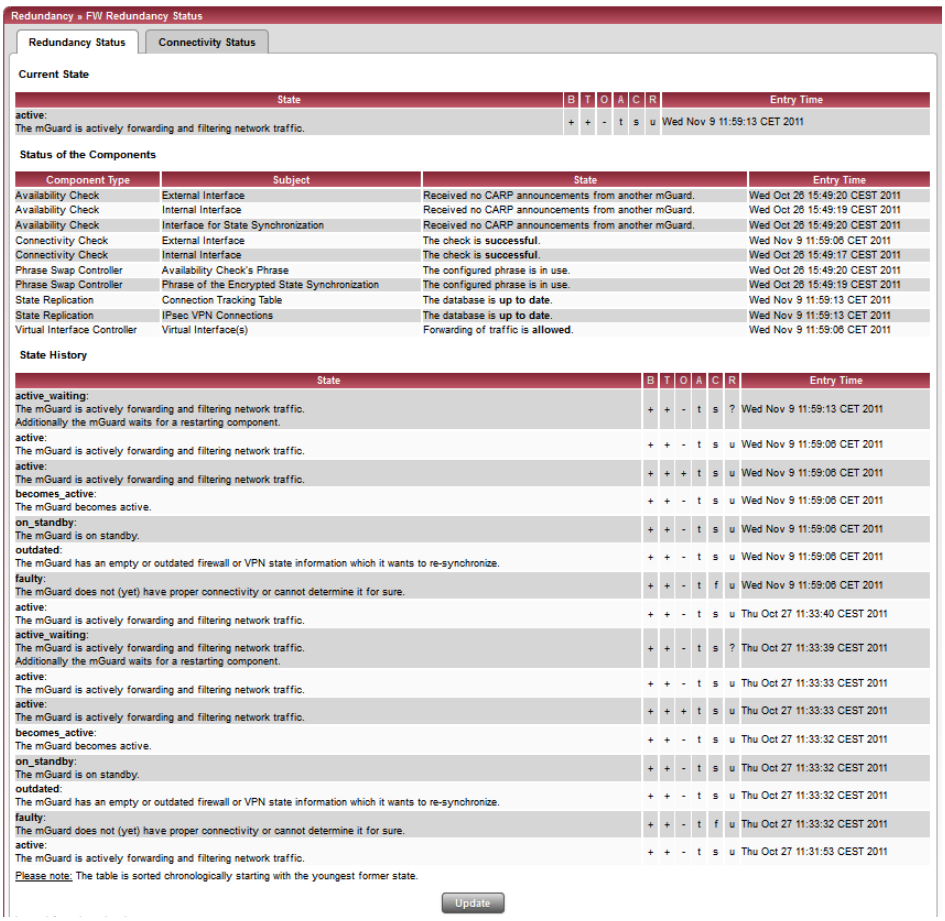

Redundancy » Firewall Redundancy
Redundancy
Connectivity Checks
External interface
Kind of check
at least one target must respond
Primary targets for ICMP echo requests (Recommended are the IPs of routers in particular of a default gateway or the real IP of the other mGuard of this redundancy pair.)
IP
172.16.66.18
10.0.0.31
Secondary targets for ICMP echo requests (Used only if the check failed for the primary targets.)
IP
10.0.0.31
10.0.0.31
Internal interface
Kind of check
at least one target must respond
Primary targets for ICMP echo requests (Recommended are the IPs of routers in particular of a default gateway or the real IP of the other mGuard of this redundancy pair.)
IP
192.168.1.1
192.168.1.31
Secondary targets for ICMP echo requests (Used only if the check failed for the primary targets.)
IP
192.168.1.31
192.168.1.31

Redundancy >> Firewall Redundancy >> Connectivity Checks		
External interface	**Kind of check**	Specifies whether a connectivity check is performed on the external interface, and if so, how. If **at least one target must respond** is selected, it does not matter whether the ICMP echo request is answered by the primary or secondary target. The request is only sent to the secondary target if the primary target did not offer a suitable answer. In this way, configurations can be supported where the devices are only provided with ICMP echo requests if required. If **all targets of one set must respond** is selected, then both targets must answer. If no secondary target is specified, then only the primary target must answer. If **Ethernet link detection only** is selected, then only the state of the Ethernet connection is checked.

Redundancy >> Firewall Redundancy >> Connectivity Checks		
	Primary targets for ICMP echo requests	This is an unsorted list of IP addresses used as targets for ICMP echo requests. We recommend using the IP addresses of routers, especially the IP addresses of default gateways or the actual IP address of the other mGuard. Default: 10.0.0.30, 10.0.0.31 (for new addresses) Each set of targets for state synchronization can contain a maximum of ten targets.
	Secondary targets for ICMP echo requests	See above Only used if the check of the primary targets has failed. Failure of a secondary target is not detected in normal operation. Default: 10.0.0.30 (10.0.0.31 for new addresses) Each set of targets for state synchronization can contain a maximum of ten targets.
Internal interface	**Kind of check**	Specifies whether a connectivity check is performed on the internal interface, and if so, how. The settings are the same as those for the external interface.
	Primary targets for ICMP echo requests	See above Factory default: 192.168.1.30 (192.168.1.31 for new addresses)
	Secondary targets for ICMP echo requests	See above Factory default: 192.168.1.30 (192.168.1.31 for new addresses)

13.2 Redundancy >> FW Redundancy Status

13.2.1 Redundancy Status



Redundancy » FW Redundancy Status

Redundancy Status | Connectivity Status

Current State

State	B	T	O	A	C	R	Entry Time
active: The mGuard is actively forwarding and filtering network traffic.	+	+	-	t	s	u	Wed Nov 9 11:59:13 CET 2011

Status of the Components

Component Type	Subject	State	Entry Time
Availability Check	External Interface	Received no CARP announcements from another mGuard.	Wed Oct 26 15:49:20 CEST 2011
Availability Check	Internal Interface	Received no CARP announcements from another mGuard.	Wed Oct 26 15:49:19 CEST 2011
Availability Check	Interface for State Synchronization	Received no CARP announcements from another mGuard.	Wed Oct 26 15:49:20 CEST 2011
Connectivity Check	External Interface	The check is **successful**.	Wed Nov 9 11:59:06 CET 2011
Connectivity Check	Internal Interface	The check is **successful**.	Wed Oct 26 15:49:17 CEST 2011
Phrase Swap Controller	Availability Check's Phrase	The configured phrase is in use.	Wed Oct 26 15:49:20 CEST 2011
Phrase Swap Controller	Phrase of the Encrypted State Synchronization	The configured phrase is in use.	Wed Oct 26 15:49:19 CEST 2011
State Replication	Connection Tracking Table	The database is **up to date**.	Wed Nov 9 11:59:13 CET 2011
State Replication	IPsec VPN Connections	The database is **up to date**.	Wed Nov 9 11:59:13 CET 2011
Virtual Interface Controller	Virtual Interface(s)	Forwarding of traffic is **allowed**.	Wed Nov 9 11:59:06 CET 2011

State History

State	B	T	O	A	C	R	Entry Time
active_waiting: The mGuard is actively forwarding and filtering network traffic. Additionally the mGuard waits for a restarting component.	+	+	-	t	s	?	Wed Nov 9 11:59:13 CET 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	-	t	s	u	Wed Nov 9 11:59:06 CET 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	+	t	s	u	Wed Nov 9 11:59:06 CET 2011
becomes_active: The mGuard becomes active.	+	+	-	t	s	u	Wed Nov 9 11:59:06 CET 2011
on_standby: The mGuard is on standby.	+	+	-	t	s	u	Wed Nov 9 11:59:06 CET 2011
outdated: The mGuard has an empty or outdated firewall or VPN state information which it wants to re-synchronize.	+	+	-	t	s	u	Wed Nov 9 11:59:06 CET 2011
faulty: The mGuard does not (yet) have proper connectivity or cannot determine it for sure.	+	+	-	t	f	u	Wed Nov 9 11:59:06 CET 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	-	t	s	u	Thu Oct 27 11:33:40 CEST 2011
active_waiting: The mGuard is actively forwarding and filtering network traffic. Additionally the mGuard waits for a restarting component.	+	+	-	t	s	?	Thu Oct 27 11:33:39 CEST 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	-	t	s	u	Thu Oct 27 11:33:33 CEST 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	+	t	s	u	Thu Oct 27 11:33:33 CEST 2011
becomes_active: The mGuard becomes active.	+	+	-	t	s	u	Thu Oct 27 11:33:32 CEST 2011
on_standby: The mGuard is on standby.	+	+	-	t	s	u	Thu Oct 27 11:33:32 CEST 2011
outdated: The mGuard has an empty or outdated firewall or VPN state information which it wants to re-synchronize.	+	+	-	t	s	u	Thu Oct 27 11:33:32 CEST 2011
faulty: The mGuard does not (yet) have proper connectivity or cannot determine it for sure.	+	+	-	t	f	u	Thu Oct 27 11:33:32 CEST 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	-	t	s	u	Thu Oct 27 11:31:53 CEST 2011

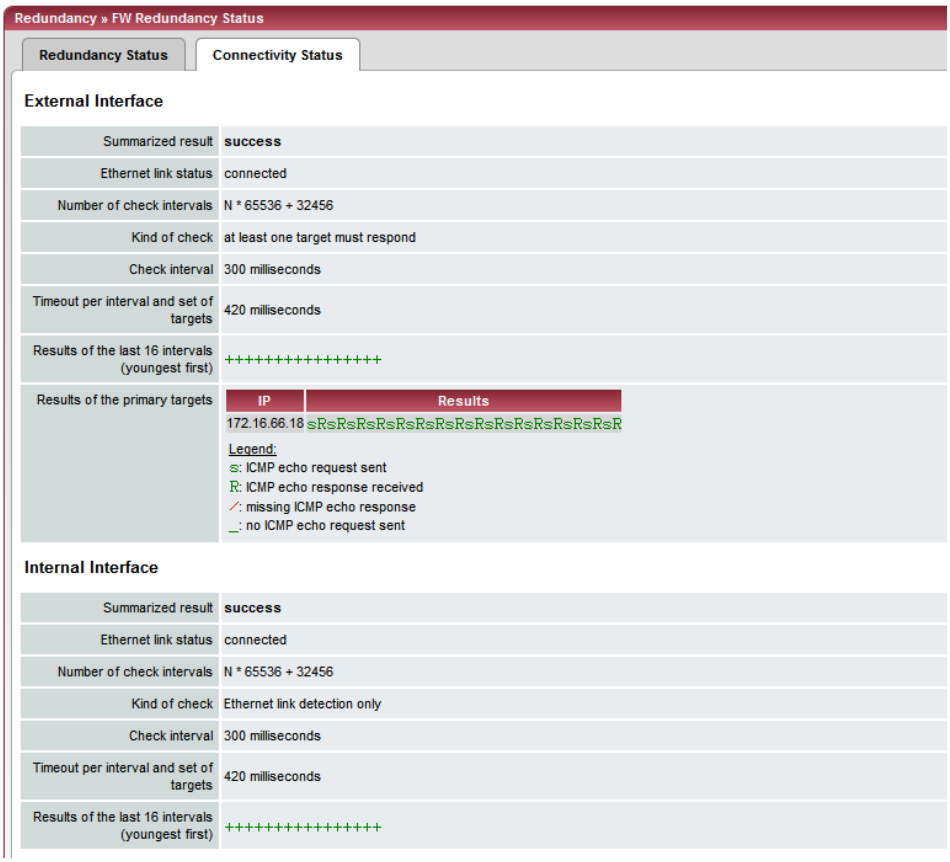
Please note: The table is sorted chronologically starting with the youngest former state.

Update

Redundancy >> FW Redundancy Status >> Redundancy Status		
Current State		Possible states: *booting*: the mGuard is starting. *faulty*: the mGuard is not (yet) connected properly. *outdated*: state synchronization of the databases is not (yet) up-to-date. *on_standby*: the mGuard is ready for activation if the other mGuard fails. *becomes_active*: the mGuard is becoming active because the other mGuard has failed. *active*: the mGuard is active. *becomes_standby*: the mGuard is switching from the active state to standby mode. The state is changed to *outdated* since the status database has to be updated first.
Status of the Components	**Availability Check**	Relates to the status of the availability check for the internal or external interface. The availability check has three possible results. – Presence notifications (CARP) are not received from any other mGuard device. – Another mGuard is available which is to become or remain active. – Another mGuard is available which is active but is to go “on_standby”.
	Connectivity Checks	Indicates whether the check was successful. Each interface is checked separately.
	State Replication	When synchronizing the state, various databases are checked to see whether everything is up-to-date. With one redundant pair, only one database is active while the other is on standby. Any change made to this state is also displayed. – The **Connection Tracking Table** relates to the firewall state database. – **IPsec VPN Connections** (with activated VPN redundancy)
	Virtual Interface Controller	All virtual interfaces are checked together to see whether the forwarding of packets is allowed.

Redundancy >> FW Redundancy Status >> Redundancy Status				
State History			The table starts with the most recent state.	
			The abbreviations are as follows:	
	B	**Firmware status**	**+**	Firmware started up completely
			-	Firmware not yet started up completely
	T	**System time**	**+**	Valid system time
			-	Invalid system time
	O	**Timeout of the previous state**	**+**	Timeout
			-	No timeout
	A	**Availability check**	**?**	Unknown state
			s	Another mGuard is available. This mGuard is active (or is currently being enabled).
			f	Another mGuard is available. This mGuard is on standby (or is currently switching to standby).
			t	No other mGuard available
	C	**Connectivity check**	**?**	Unknown state
			s	Check of all components was successful
			f	Check of at least one component has failed
	R	**State synchronization**	**?**	Unknown state
			u	Database is up-to-date
			o	Database is obsolete
			-	Database switching to “on_standby”
			+	Database switching to “active”

13.2.2 Connectivity Status



Redundancy >> FW Redundancy Status >> Connectivity Status		
External Interface	**Summarized result**	**success/fail** Result of the connectivity check for the external interface. The **fail** result is also displayed until the specific result of the connectivity check is known. The last two intervals of the connectivity check are taken into consideration for the combined result. **success** is only displayed if both were successful. **success (longer due to waiting time)** is displayed, if the time an error was present was shorter than set under *"Waiting time prior to switching"* in the *Redundancy >> Firewall Redundancy >> Redundancy* menu.
	Ethernet link status	Shows whether the Ethernet connection has been established.
	Number of check intervals	Number of completed check intervals. When the counter is full, a message is displayed in front of the number.
	Kind of check	Repeats the setting for the connectivity check (see *Kind of check* on Page 313).

Redundancy >> FW Redundancy Status >> Connectivity Status		
	Check interval	Shows the time (in milliseconds) between the starts of the checks. This value is calculated from the set fail-over switching time.
	Timeout per interval and set of targets	Shows the time (in milliseconds) after which a target is classed as “no response” if no response to the ICMP echo request has been received. This value is calculated from the set fail-over switching time.
	Waiting time prior to reporting an error (except for link errors)	Time the redundancy system ignores an error. The connectivity and availability checks ignore an error until it is still present after the time set here has elapsed. This value is set under *“Waiting time prior to switching”* in the *Redundancy >> Firewall Redundancy >> Redundancy* menu.
	Results of the last 16 intervals (youngest first)	A green plus indicates a successful check. A red minus indicates a failed check.
	Results of the primary targets	Only visible when a primary target is set (see *Primary targets for ICMP echo requests* on Page 313). Shows the results of the ICMP echo requests in chronological order. The most recent result is at the front. “sR” indicates a cycle during which ICMP echo requests have been correctly transmitted and received. Missing answers are indicated by a “/” and requests that have not been transmitted are indicated by a “_”.
	Results of the secondary targets	Only visible when a secondary target is set (see *Secondary targets for ICMP echo requests* on Page 313).
Internal Interface	**Summarized result**	See *External Interface*
	Ethernet link status	See *External Interface*
	Number of check intervals	See *External Interface*
	Check interval	See *External Interface*
	Timeout per interval and set of targets	See *External Interface*
	Results of the last 16 intervals (youngest first)	See *External Interface*

13.3 Ring/Network Coupling

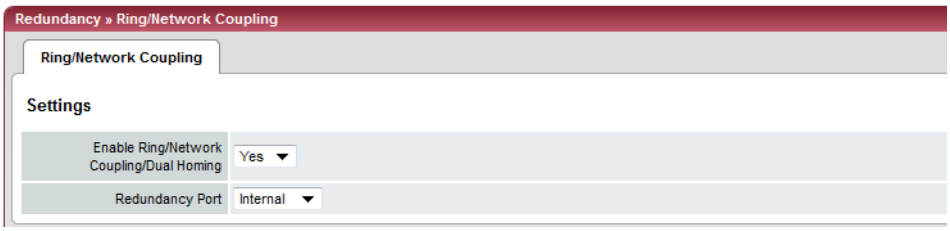
The ring/network coupling function is **not** supported on by *mGuard centerport*.

Ring/network coupling with restrictions:

– mGuard delta: the internal side (switch ports) cannot be switched off

– mGuard pci: in driver mode, the internal network interface cannot be switched off (however, this is possible in power-over-PCI mode)

13.3.1 Ring/Network Coupling



Redundancy >> Firewall Redundancy >> Ring/Network Coupling		
Settings	**Enable Ring/Network Coupling/Dual Homing**	**Yes/No** When activated, the status of the Ethernet connection is transmitted from one port to another in Stealth mode. This means that interruptions in the network can be traced easily.
	Redundancy Port	**Internal/External** **Internal**: if the connection is lost/established on the LAN port, the WAN port is also disabled/enabled. **External**: if the connection is lost/established on the WAN port, the LAN port is also disabled/enabled.

14 Logging menu

Logging refers to the recording of event messages, e.g., regarding settings that have been made, the application of firewall rules, errors, etc.

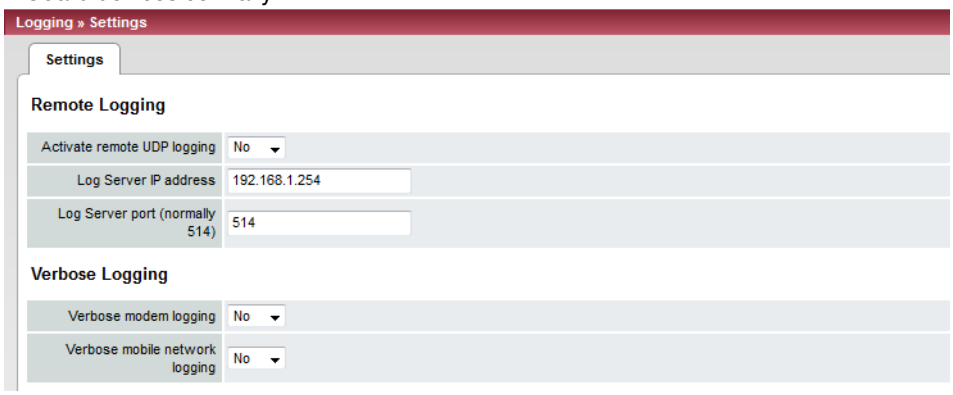
Log entries are recorded in various categories and can be sorted and displayed according to these categories (see “Logging >> Browse local logs” on page 323).

14.1 Logging >> Settings

14.1.1 Settings

All log entries are recorded in the RAM of the mGuard by default. Once the maximum memory space for log entries has been used up, the oldest log entries are automatically overwritten by new entries. In addition, all log entries are deleted when the mGuard is switched off.

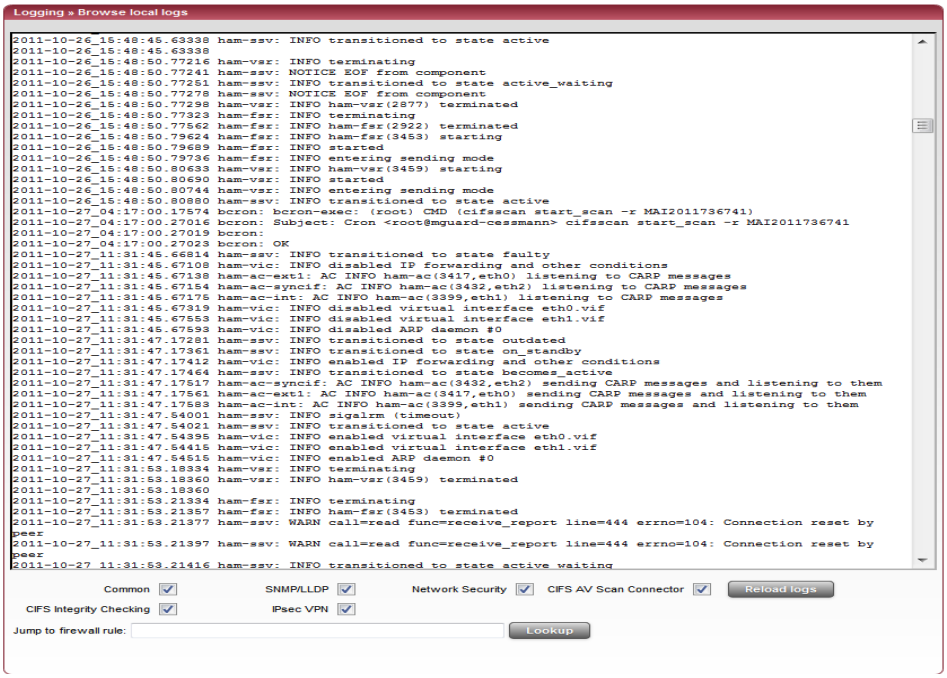
To prevent this, log entries (SysLog messages) can be transmitted to an external computer (SysLog server). This is particularly useful if you wish to manage the logs of multiple mGuard devices centrally.



Logging >> Settings		
Remote Logging	**Activate remote UDP logging**	**Yes/No** If you want all log entries to be transmitted to the external log server (specified below), select **Yes**.
	Log Server IP address	Specify the IP address of the log server to which the log entries should be transmitted via UDP. An IP address must be specified, not a host name. This function does not support name resolution because it might not be possible to make log entries if a DNS server failed.
	Log Server port	Specify the port of the log server to which the log entries should be transmitted via UDP. Default: 514

Logging >> Settings		
		If SysLog messages should be transmitted to a SysLog server via a VPN channel, the IP address of the SysLog server must be located in the network that is specified as the **Remote** network in the definition of the VPN connection. The internal IP address must be located in the network that is specified as **Local** in the definition of the VPN connection (see IPsec VPN >> Connections >> Edit >> General). – If the IPsec VPN >> Connections >> Edit >> General, **Local** option is set to **1:1 NAT** (see Page 263), the following applies: The internal IP address must be located in the specified local network. – If the IPsec VPN >> Connections >> Edit >> General, **Remote** option is set to **1:1 NAT** (see Page 265), the following applies: The IP address of the SysLog server must be located in the network that is specified as **Remote** in the definition of the VPN connection.
Verbose Logging	**Verbose modem logging**	Only available if an internal or external modem is available and switched on. – Internal modem: mGuard rs4000/rs2000 3G, mGuard industrial rs with internal analog modem or ISDN modem – External modem: mGuard rs4000/rs2000, mGuard rs4000/rs2000 3G, mGuard centerport, mGuard industrial rs, mGuard blade, mGuard delta, mGuard delta^2, EAGLE mGuard Verbose logging
	Verbose mobile network logging	Only available with the mGuard rs4000/rs2000 3G. Verbose logging

14.2 Logging >> Browse local logs


Logging » Browse local logs
2011-10-26_15:48:45.63338 ham-ssv: INFO transitioned to state active
2011-10-26_15:48:45.63338
2011-10-26_15:48:50.77216 ham-vsr: INFO terminating
2011-10-26_15:48:50.77241 ham-ssv: NOTICE EOF from component
2011-10-26_15:48:50.77251 ham-ssv: INFO transitioned to state active_waiting
2011-10-26_15:48:50.77278 ham-ssv: NOTICE EOF from component
2011-10-26_15:48:50.77298 ham-vsr: INFO ham-vsr(2877) terminated
2011-10-26_15:48:50.77323 ham-fsr: INFO terminating
2011-10-26_15:48:50.77562 ham-fsr: INFO ham-fsr(2922) terminated
2011-10-26_15:48:50.79624 ham-fsr: INFO ham-fsr(3453) starting
2011-10-26_15:48:50.79689 ham-fsr: INFO started
2011-10-26_15:48:50.79736 ham-fsr: INFO entering sending mode
2011-10-26_15:48:50.80633 ham-vsr: INFO ham-vsr(3459) starting
2011-10-26_15:48:50.80690 ham-vsr: INFO started
2011-10-26_15:48:50.80744 ham-vsr: INFO entering sending mode
2011-10-26_15:48:50.80880 ham-ssv: INFO transitioned to state active
2011-10-27_04:17:00.17574 bcron: bcron-exec: (root) CMD (cifsscan start_scan -r MAI2011736741)
2011-10-27_04:17:00.27016 bcron: Subject: Cron <root@mguard-cessmann> cifsscan start_scan -r MAI2011736741
2011-10-27_04:17:00.27019 bcron:
2011-10-27_04:17:00.27023 bcron: OK
2011-10-27_11:31:45.66814 ham-ssv: INFO transitioned to state faulty
2011-10-27_11:31:45.67108 ham-vic: INFO disabled IP forwarding and other conditions
2011-10-27_11:31:45.67138 ham-ac-ext1: AC INFO ham-ac(3417,eth0) listening to CARP messages
2011-10-27_11:31:45.67154 ham-ac-syncif: AC INFO ham-ac(3432,eth2) listening to CARP messages
2011-10-27_11:31:45.67175 ham-ac-int: AC INFO ham-ac(3399,eth1) listening to CARP messages
2011-10-27_11:31:45.67319 ham-vic: INFO disabled virtual interface eth0.vif
2011-10-27_11:31:45.67553 ham-vic: INFO disabled virtual interface eth1.vif
2011-10-27_11:31:45.67593 ham-vic: INFO disabled ARP daemon #0
2011-10-27_11:31:47.17281 ham-ssv: INFO transitioned to state outdated
2011-10-27_11:31:47.17361 ham-ssv: INFO transitioned to state on_standby
2011-10-27_11:31:47.17412 ham-vic: INFO enabled IP forwarding and other conditions
2011-10-27_11:31:47.17464 ham-ssv: INFO transitioned to state becomes_active
2011-10-27_11:31:47.17517 ham-ac-syncif: AC INFO ham-ac(3432,eth2) sending CARP messages and listening to them
2011-10-27_11:31:47.17561 ham-ac-ext1: AC INFO ham-ac(3417,eth0) sending CARP messages and listening to them
2011-10-27_11:31:47.17583 ham-ac-int: AC INFO ham-ac(3399,eth1) sending CARP messages and listening to them
2011-10-27_11:31:47.54001 ham-ssv: INFO sigalrm (timeout)
2011-10-27_11:31:47.54021 ham-ssv: INFO transitioned to state active
2011-10-27_11:31:47.54395 ham-vic: INFO enabled virtual interface eth0.vif
2011-10-27_11:31:47.54416 ham-vic: INFO enabled virtual interface eth1.vif
2011-10-27_11:31:47.54516 ham-vic: INFO enabled ARP daemon #0
2011-10-27_11:31:53.18334 ham-vsr: INFO terminating
2011-10-27_11:31:53.18360 ham-vsr: INFO ham-vsr(3459) terminated
2011-10-27_11:31:53.18360
2011-10-27_11:31:53.21334 ham-fsr: INFO terminating
2011-10-27_11:31:53.21357 ham-fsr: INFO ham-fsr(3453) terminated
2011-10-27_11:31:53.21377 ham-ssv: WARN call=read func=receive_report line=444 errno=104: Connection reset by peer
2011-10-27_11:31:53.21397 ham-ssv: WARN call=read func=receive_report line=444 errno=104: Connection reset by peer
2011-10-27_11:31:53.21416 ham-ssv: INFO transitioned to state active_waiting
Common
SNMP/LLDP
Network Security
CIFS AV Scan Connector
Reload logs
CIFS Integrity Checking
IPsec VPN
Jump to firewall rule:
Lookup

The corresponding checkboxes for filtering entries according to their category are displayed below the log entries, depending on which mGuard functions were active.

To display one or more categories, enable the checkboxes for the desired categories and click on **Reload logs**.

14.2.1 Log entry categories

Common

Log entries that cannot be assigned to other categories.

Network Security

In the case of the **mGuard rs2000** and **mGuard rs2000 3G**, access via its firewall is **not** logged.

Logged events are shown here if the logging of events was selected when defining the firewall rules (Log = Yes).

Log ID and number for tracing errors

Log entries that relate to the firewall rules listed below have a log ID and number. This log ID and number can be used to trace the firewall rule to which the corresponding log entry relates and that led to the corresponding event.

Firewall rules and their log ID

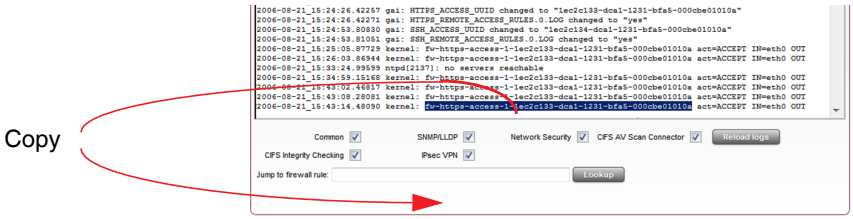
- Packet filters:
  Network Security >> Packet Filter >> Incoming Rules menu
  Network Security >> Packet Filter >> Outgoing Rules menu
  Log ID: *fw-incoming* or *fw-outgoing*
- Firewall rules for VPN connections:
  IPsec VPN >> Connections >> Edit >> Firewall menu, Incoming/Outgoing
  Log ID: *vpn-fw-in* or *vpn-fw-out*
- Firewall rules for web access to the mGuard via HTTPS:
  Management >> Web Settings >> Access menu
  Log ID: *fw-https-access*
- Firewall rules for access to the mGuard via SNMP:
  Management >> SNMP >> Query menu
  Log ID: *fw-snmp-access*
- Firewall rules for SSH remote access to the mGuard:
  Management >> System Settings >> Shell Access menu
  Log ID: *fw-ssh-access*
- Firewall rules for the user firewall:
  Network Security >> User Firewall menu, Firewall rules
  Log ID: *ufw-*
- Rules for NAT, port forwarding:
  Network >> NAT >> IP and Port Forwarding menu
  Log ID: *fw-portforwarding*
- Firewall rules for the serial interface:
  Network >> Interfaces >> Dial-in menu
  Incoming Rules
  Log ID: *fw-serial-incoming*
  Outgoing Rules
  Log ID: *fw-serial-outgoing*

Searching for firewall rules on the basis of a network security log

If the **Network Security** checkbox is enabled so that the relevant log entries are displayed, the Jump to firewall rule search field is displayed below the *Reload logs* button.

Proceed as follows if you want to trace the firewall rule referenced by a log entry in the *Network Security* category and which resulted in the corresponding event:

1. Select the section that contains the log ID and number in the relevant log entry, for example: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a


Copy
2006-08-21_15:24:26.42257 gai: HTTPS_ACCESS_UUID changed to "1ec2c133-dca1-1231-bfa5-000cbe01010a"
2006-08-21_15:24:26.42271 gai: HTTPS_REMOTE_ACCESS_RULES.0.LOG changed to "yes"
2006-08-21_15:24:53.80830 gai: SSH_ACCESS_UUID changed to "1ec2c134-dca1-1231-bfa5-000cbe01010a"
2006-08-21_15:24:53.81051 gai: SSH_REMOTE_ACCESS_RULES.0.LOG changed to "yes"
2006-08-21_15:25:05.87729 kernel: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a act=ACCEPT IN=eth0 OUT
2006-08-21_15:26:03.86944 kernel: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a act=ACCEPT IN=eth0 OUT
2006-08-21_15:33:24.99599 ntpd[2137]: no servers reachable
2006-08-21_15:34:59.15168 kernel: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a act=ACCEPT IN=eth0 OUT
2006-08-21_15:43:02.46817 kernel: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a act=ACCEPT IN=eth0 OUT
2006-08-21_15:43:08.28081 kernel: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a act=ACCEPT IN=eth0 OUT
2006-08-21_15:43:14.48090 kernel: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a act=ACCEPT IN=eth0 OUT
Common
SNMP/LLDP
Network Security
CIFS AV Scan Connector
Reload logs
CIFS Integrity Checking
IPsec VPN
Jump to firewall rule:
Lookup

2. Copy this section into the **Jump to firewall rule** field.
3. Click on **Lookup**.
   The configuration page containing the firewall rule that the log entry refers to is displayed.

Blade

In addition to error messages, the following messages are output on the mGuard blade controller:

(The areas enclosed by < and > are replaced by the relevant data in the log entries.)

General messages:

blade daemon "<version>" starting ...
Blade[<bladenr>] online
Blade[<bladenr>] is mute
Blade[<bladenr>] not running
Reading timestamp from blade[<bladenr>]

When activating a configuration profile on a blade:

Push configuration to blade[<bladenr>]
reconfiguration of blade[<bladenr>] returned <returncode>
blade[<bladenr>] # <text>

When retrieving a configuration profile from a blade:

Pull configuration from blade[<bladenr>]
Pull configuration from blade[<bladenr>] returned <returncode>

CIFS AV Scan Connector

This log contains CIFS server messages. This server is used by the mGuard itself for share purposes.

In addition, messages that occur when connecting the network drives and are grouped together and provided by the CIFS server are also visible.

CIFS Integrity Checking

Messages relating to the integrity check of network drives are displayed in this log.

In addition, messages that occur when connecting the network drives and are required for the integrity check are also visible.

DHCP server/relay

Messages from the services defined under “Network -> DHCP”.

SNMP/LLDP

Messages from services defined under “Management -> SNMP”.

IPsec VPN

Lists all VPN events.

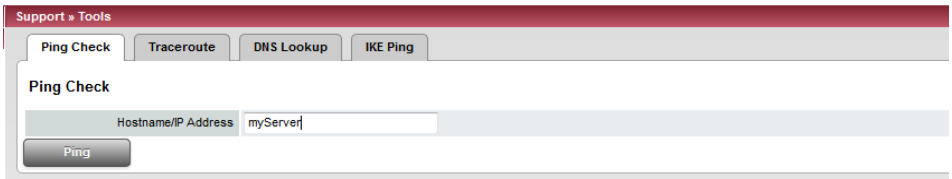
The format corresponds to standard Linux format.

There are special evaluation programs that present information from the logged data in a more easily readable format.

15 Support menu

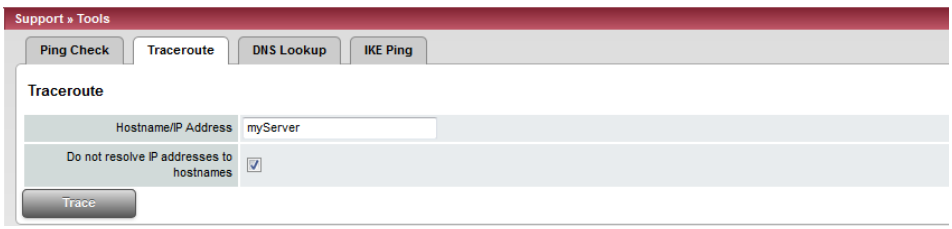
15.1 Support >> Tools

15.1.1 Ping Check



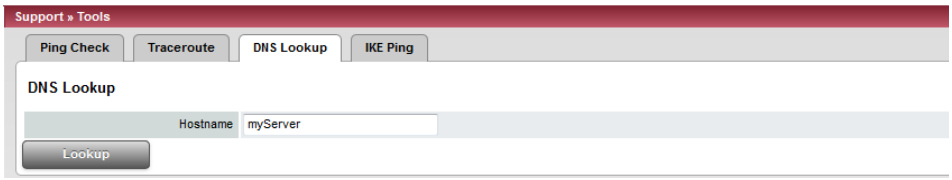
Support >> Tools >> Ping Check	
Ping Check	**Aim**: to check whether a partner can be accessed via a network. **Procedure**: • Enter the IP address or host name of the partner in the **Hostname/IP Address** field. Then click on **Ping**. A corresponding message is then displayed.

15.1.2 Traceroute



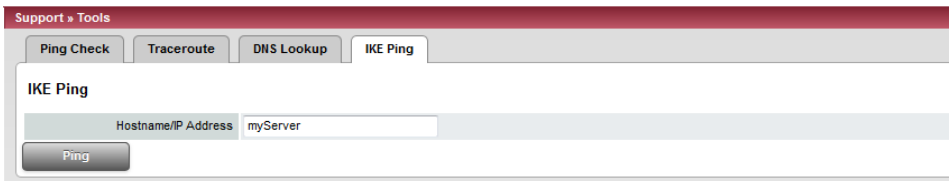
Support >> Tools >> Traceroute	
Traceroute	**Aim**: to determine which intermediate points or routers are located on the connection path to a partner. **Procedure**: • Enter the host name or IP address of the partner whose route is to be determined in the **Hostname/IP Address** field. • If the points on the route are to be output with IP addresses instead of host names (if applicable), activate the **Do not resolve IP addresses to hostnames** checkbox. • Then click on **Trace**. A corresponding message is then displayed.

15.1.3 DNS Lookup



Support >> Tools >> DNS Lookup	
DNS Lookup	**Aim**: to determine which host name belongs to a specific IP address or which IP address belongs to a specific host name. **Procedure**: • Enter the IP address or host name in the **Hostname** field. • Click on **Lookup**. The response, which is determined by the mGuard according to the DNS configuration, is then returned.

15.1.4 IKE Ping

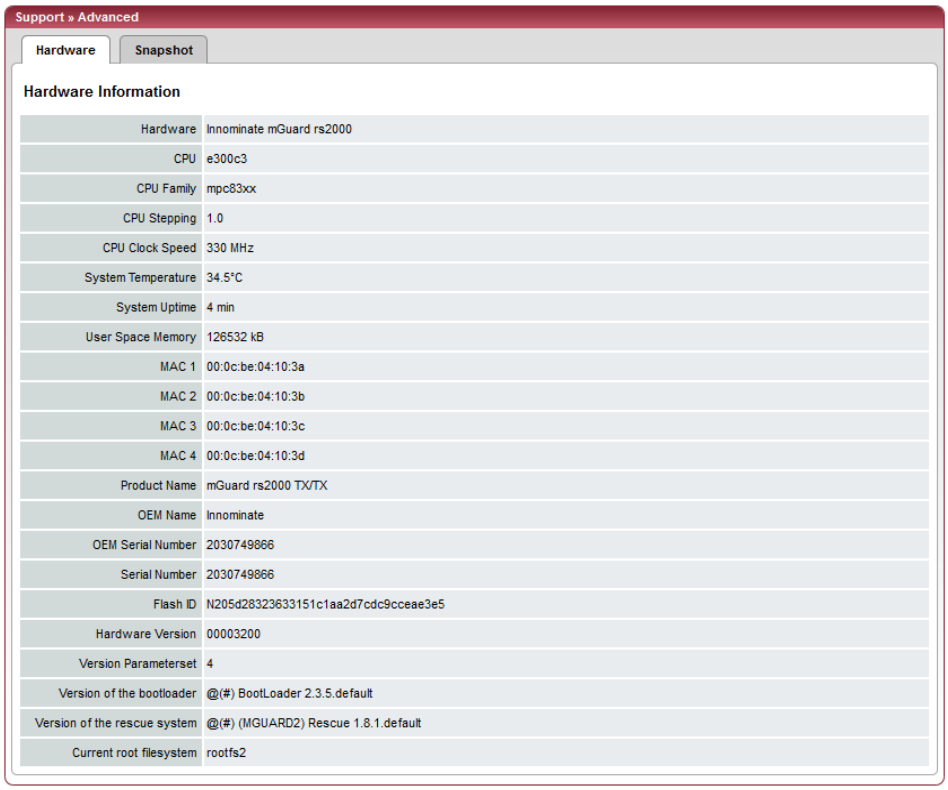


Support >> Tools >> IKE Ping	
IKE Ping	**Aim**: to determine whether the VPN software for a VPN gateway is able to establish a VPN connection, or whether a firewall prevents this, for example. **Procedure**: • Enter the name or IP address of the VPN gateway in the **Hostname/IP Address** field. • Click on **Ping**. • A corresponding message is then displayed.

15.2 Support >> Advanced

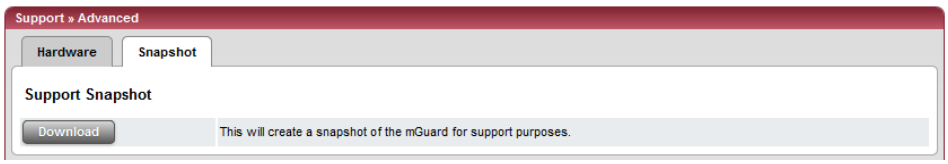
15.2.1 Hardware

This page lists various hardware properties of the mGuard.



15.2.2 Snapshot

This function is used for support purposes.



It creates a compressed file (in tar.gz format) containing all active configuration settings and log entries that could be relevant for error diagnostics.

This file does not contain any private information such as private machine certificates or passwords. However, any pre-shared keys of VPN connections are contained in the snapshots.

To create a snapshot, proceed as follows:

- Click on **Download**.
- Save the file (under the name “snapshot.tar.gz”).

Provide the file to the support team of your dealer, if required.

16 Redundancy

The firewall and VPN redundancy functions are **not** available on the **mGuard rs2000** and **mGuard rs2000 3G**.

There are several different ways of compensating for errors using the mGuard so that an existing connection is not interrupted.

– **Firewall redundancy:** two identical mGuard devices can be combined to form a redundant pair, meaning one takes over the functions of the other if an error occurs.
– **VPN redundancy**: an existing firewall redundancy forms the basis for VPN redundancy. In addition, the VPN connections are designed so that at least one mGuard in a redundant pair operates the VPN connections.
– **Ring/network coupling**: in ring/network coupling, another method is used. Parts of a network are designed as redundant. In the event of errors, the alternative path is selected.

16.1 Firewall redundancy

Using firewall redundancy, it is possible to combine two identical mGuard devices into a redundant pair (single virtual router). One mGuard takes over the functions of the other if an error occurs. Both mGuard devices run synchronously, meaning an existing connection is not interrupted when the device is switched.

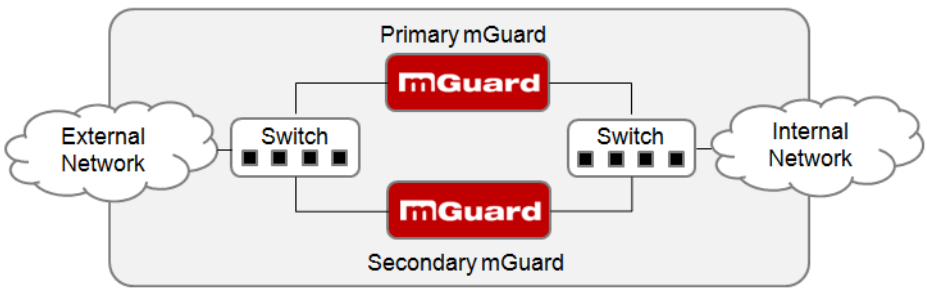


Figure 16-1 Firewall redundancy (example)

Basic requirements for firewall redundancy

A license is required for the firewall redundancy function. It can only be used if the corresponding license has been purchased and installed.

– Only identical mGuard devices can be used together in a redundant pair.
– In Router network mode, firewall redundancy is only supported with the “static” Router mode.
– The Stealth network mode is currently not supported.
– For further restrictions, see “Requirements for firewall redundancy” on page 334 and “Limits of firewall redundancy” on page 344.

16.1.1 Components in firewall redundancy

Firewall redundancy is comprised of several components:

– **Connectivity check**
  Checks whether the necessary network connections have been established.
– **Availability check**
  Checks whether an active mGuard is available and whether this should remain active.
– **State synchronization of the firewall**
  The mGuard on standby receives a copy of the current firewall database state.
– **Virtual network interface**
  Provides virtual IP addresses and MAC addresses that can be used by other devices as routes and default gateways.
– **State monitoring**
  Coordinates all components.
– **Status indicator**
  Shows the user the state of the mGuard.

Connectivity check

On each mGuard in a redundant pair, checks are constantly made as to whether a connection is established through which the network packets can be forwarded.

Each mGuard checks its own internal and external network interfaces independently of each other. Both interfaces are tested for a continuous connection. This connection must be in place, otherwise the connectivity check will fail.

ICMP echo requests can also be sent (optional). The ICMP echo requests can be set using the *Redundancy >> Firewall Redundancy >> Connectivity Checks* menu.

Availability check

On each mGuard in a redundant pair, checks are also constantly performed to determine whether an active mGuard is available and whether it should remain active. A variation of the CARP (Common Address Redundancy Protocol) is used here.

The active mGuard constantly sends presence notifications through its internal and external network interface while both mGuard devices listen. If a dedicated Ethernet link for state synchronization of the firewall is available, the presence notification is also sent via this link. In this case, the presence notification for the external network interface can also be suppressed.

The availability check fails if an mGuard does not receive any presence notifications within a certain time. The check also fails if an mGuard receives presence notifications with a lower priority than its own.

The data is always transmitted through the physical network interface and never through the virtual network interface.

State synchronization

The mGuard on standby receives a copy of the state of the mGuard that is currently active.

This includes a database containing the forwarded network connections. This database is filled and updated constantly by the forwarded network packets. It is protected against unauthorized access. The data is transmitted through the physical LAN interface and never through the virtual network interface.

To keep internal data traffic to a minimum, a VLAN can be configured to store the synchronization data in a separate multicast and broadcast domain.

Virtual IP addresses

Each mGuard is configured with virtual IP addresses. The number of virtual IP addresses depends on the network mode used. Both mGuard devices in a redundant pair must be assigned the same virtual IP addresses. The virtual IP addresses are required by the mGuard to establish virtual network interfaces.

Two virtual IP addresses are required in Router network mode, while others can be created. One virtual IP address is required for the external network interface and the other for the internal network interface.

These IP addresses are used as a gateway for routing devices located in the external or internal LAN. In this way, the devices can benefit from the high availability resulting from the use of both redundant mGuard devices.

The redundant pair automatically defines MAC addresses for the virtual network interface. These MAC addresses are identical for the redundant pair. In Router network mode, both mGuard devices share a MAC address for the virtual network interface connected to the external and internal Ethernet segment.

In Router network mode, the mGuard devices support forwarding of special UDP/TCP ports from a virtual IP address to other IP addresses, provided the other IP addresses can be reached by the mGuard. In addition, the mGuard also masks data with virtual IP addresses when masquerading rules are set up.

State monitoring

State monitoring is used to determine whether the mGuard is active, on standby or has an error. Each mGuard determines its own state independently, based on the information provided by other components. State monitoring ensures that two mGuard devices are not active at the same time.

Status indicator

The status indicator contains detailed information on the firewall redundancy state. A summary of the state can be called up using the *Redundancy >> Firewall Redundancy >> Redundancy* or *Redundancy >> Firewall Redundancy >> Connectivity Checks* menus.

16.1.2 Interaction of the firewall redundancy components

During operation, the components work together as follows: both mGuard devices perform ongoing connectivity checks for both of their network interfaces (internal and external). In addition, an ongoing availability check is performed. Each mGuard listens continuously for presence notifications (CARP) and the active mGuard also sends them.

Based on the information from the connectivity and availability checks, the state monitoring function is made aware of the state of the mGuard devices. State monitoring ensures that the active mGuard mirrors its data onto the other mGuard (state synchronization).

16.1.3 Firewall redundancy settings from previous versions

Existing configuration profiles on firmware version 6.1.x (and earlier) can be imported with certain restrictions. For information, please contact Innominate.

16.1.4 Requirements for firewall redundancy

– To use the redundancy function, both mGuards must have the same firmware.
– The firewall redundancy function can only be activated when a valid license key is installed.

  (See under: *Redundancy >> Firewall Redundancy >> Redundancy >> Enable redundancy)*
– *Redundancy >> Firewall Redundancy >> Redundancy >> Interface which is used for state synchronization*

  The **Dedicated interface** value is only accepted on mGuards which have more than two physical and separate Ethernet interfaces. This is currently the *mGuard centerport*.
– Each set of targets for the connectivity check can contain more than ten targets (A failover time cannot be guaranteed without an upper limit).

  Redundancy >> Firewall Redundancy >> Redundancy
  – *>> External interface >> Primary targets for ICMP echo requests*
  – *>> External interface >> Secondary targets for ICMP echo requests*
  – *>> Internal interface >> Primary targets for ICMP echo requests*
  – *>> Internal interface >> Secondary targets for ICMP echo requests*

  If “at least one target must respond” or “all targets of one set must respond” is selected under *External interface >> Kind of check*, then *External interface >> Primary targets for ICMP echo requests* cannot be left empty. This also applies to the internal interface.
– In **Router network mode**, at least one external and one internal virtual IP address must be set. A virtual IP address cannot be listed twice.

16.1.5 Fail-over switching time

The mGuard calculates the intervals for the connectivity check and availability check automatically according to the variables under **Fail-over switching time**.

Connectivity check

The factors which define the intervals for the connectivity check are specified in Table 16-1 on Page 335.

64-kbyte ICMP echo requests are sent for the connectivity check. They are sent on layer 3 of the Internet protocol. When VLAN is not used, 18 bytes for the MAC header and checksum are added to this with the Ethernet on layer 2. The ICMP echo reply is the same size.

The bandwidth is also shown in Table 16-1. This takes into account the values specified for a single target and adds up the bytes for the ICMP echo request and reply.

The timeout on the mGuard following transmission includes the following:

– The time required by the mGuard to transmit an ICMP echo reply. If other data traffic is expected, the half-duplex mode is not suitable here.
– The time required for the transmission of the ICMP echo request to a target. Consider the latency during periods of high capacity utilization. This applies especially when routers forward the request. The actual latency may be twice the value of the configured latency in unfavorable circumstances (connectivity check error).
– The time required on each target for processing the request and transmitting the reply to the Ethernet layer. Please note that the full-duplex mode is also used here.
– The time for transmission of the ICMP echo reply to the mGuard.

Table 16-1 Frequency of the ICMP echo requests

Fail-over switching time	ICMP echo requests per target	Timeout on the mGuard after transmission	Bandwidth per target
1 s	10 per second	100 ms	6560 bps
3 s	3.3 per second	300 ms	2187 bps
10 s	1 per second	1 s	656 bps

If secondary targets are configured, then additional ICMP echo requests may occasionally be sent to these targets. This must be taken into account when calculating the ICMP echo request rate.

The timeout for a single ICMP echo request is displayed in Table 16-1. This does not indicate how many of the responses can be missed before the connectivity check fails. The check tolerates a negative result for one of two back-to-back intervals.

Availability check

Presence notifications (CARP) measure up to 76 bytes on layer 3 of the Internet protocol. When VLAN is not used, 18 bytes for the MAC header and checksum are added to this with the Ethernet on layer 2. The ICMP echo reply is the same size.

Table 16-2 shows the maximum frequency at which the presence notifications (CARP) are sent from the active mGuard. It also shows the bandwidth used in the process. The frequency depends on the mGuard priority and the *Fail-over switching time*.

Table 16-2 also shows the maximum latency tolerated by the mGuard for the network that is used to transmit the presence notifications (CARP). If this latency is exceeded, the redundant pair can exhibit undefined behavior.

Table 16-2 Frequency of the presence notifications (CARP)

Fail-over switching time	Presence notifications (CARP) per second		Maximum latency	Bandwidth on layer 2 for the high priority
	High priority	Low priority		
1 s	50 per second	25 per second	20 ms	37600 bps
3 s	16.6 per second	8.3 per second	60 ms	12533 bps
10 s	5 per second	2.5 per second	200 ms	3760 bps

16.1.6 Error compensation through firewall redundancy

Firewall redundancy is used to compensate for hardware failures.

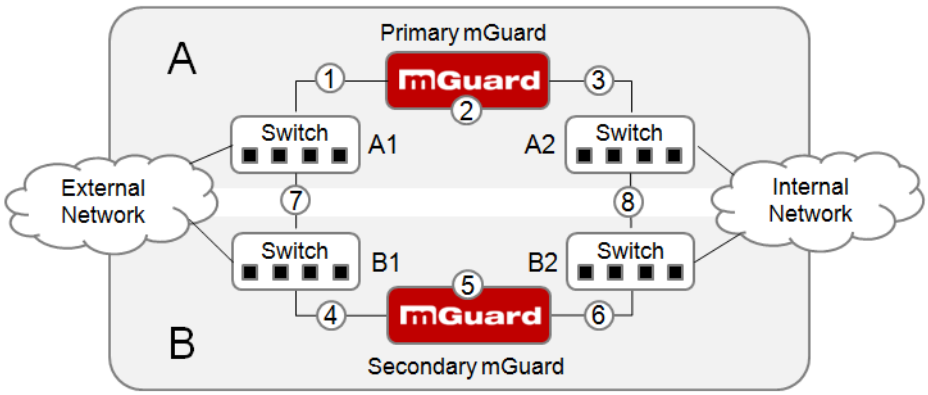


Figure 16-2 Possible error locations (1 ... 8)

Figure 16-2 shows a diagram containing various error locations (not related to the network mode)

Each of the mGuard devices in a redundant pair is located in a different area (A and B). The mGuard in area A is connected to switch A1 through its external Ethernet interface and to switch A2 through its internal Ethernet interface. mGuard B is connected accordingly to switches B1 and B2. In this way, the switches and mGuard devices connect an external Ethernet network to an internal Ethernet network. The connection is established by forwarding network packets (in Router network mode).

Firewall redundancy compensates for errors displayed in Figure 16-2 if only one occurs at any given time. If two errors occur simultaneously, they are only compensated if they occur in the same area (A or B).

For example, if one of the mGuard devices fails completely due to a power outage, then this is detected. A connection failure is compensated if the connection fails completely or partially. When the connectivity check is set correctly, a faulty connection caused by the loss of data packets or an excessive latency is detected and compensated. Without the connectivity check, the mGuard cannot determine which area caused the error.

A connection failure between switches on a network side (internal/external) is not compensated for (7 and 8 in Figure 16-2).

16.1.7 Handling firewall redundancy in extreme situations

The situations described here only occur rarely.

Restoration in the event of a network lobotomy

A network lobotomy occurs if a redundant pair is separated into two mGuard devices operating independently of one another. In this case, each mGuard deals with its own tracking information as the two mGuard devices can no longer communicate via layer 2. A network lobotomy can be triggered by a rare and unfortunate combination of network settings, network failures, and firewall redundancy settings.

Each mGuard is active during a network lobotomy. The following occurs after the network lobotomy has been rectified: if the mGuard devices have different priorities, the device with the higher priority becomes active and the other switches to standby. If both mGuard devices have the same priority, an identifier sent with the presence notifications (CARP) determines which mGuard becomes active.

Both mGuard devices manage their own firewall state during the network lobotomy. The active mGuard retains its state. Connections on the other mGuard, which were established during the lobotomy, are dropped.

Fail-over when establishing complex connections

Complex connections are network protocols which are based on different IP connections. One example of this is the FTP protocol. In an FTP protocol, the client establishes a control channel for a TCP connection. The server is then expected to open another TCP connection over which the client can then transmit data. The data channel on port 20 of the server is set up while the control channel on port 21 of the server is being established.

If the relevant connection tracking function is activated on the mGuard (see “Advanced” on page 216), complex connections of this type are tracked. In this case, the administrator only needs to create a firewall rule on the mGuard which allows the client to establish a control channel to the FTP server. The mGuard enables the server to establish a data channel automatically, regardless of whether the firewall rules allow for this.

The tracking of complex connections is part of the firewall state synchronization process. However, to keep the latency short, the mGuard forwards the network packets independently from the firewall state synchronization update that has been triggered by the network packets themselves.

Therefore, it may be the case for a very brief period that a state change for the complex connection is not forwarded to the mGuard on standby if the active mGuard fails. In this case, tracking of the connection from the mGuard which is active after the fail-over is not continued correctly. This cannot be corrected by the mGuard. The data link is then reset or interrupted.

Fail-over when establishing semi-unidirectional connections

A semi-unidirectional connection refers to a single IP connection (such as UDP connections) where the data only travels in one direction after the connection is established with a bidirectional handshake.

The data flows from the responder to the initiator. The initiator only sends data packets at the very start.

The following applies only to certain protocols which are based on UDP. Data always flows in both directions on TCP connections.

If the firewall of the mGuard is set up to only accept data packets from the initiator, the firewall accepts all related responses per se. This happens regardless of whether or not a relevant firewall rule is available.

A scenario is conceivable in which the mGuard allows the initiating data packet to pass through and then fails before the relevant connection entry has been made in the other mGuard. The other mGuard may then reject the responses as soon as it becomes the active mGuard.

The mGuard cannot correct this situation due to the single-sided connection. As a countermeasure, the firewall can be configured so that the connection can be established in both directions. This is normally already handled via the protocol layer and no additional assignment is required.

Loss of data packets during state synchronization

If data packets are lost during state synchronization, this is detected automatically by the mGuard, which then requests the active mGuard to send the data again.

This request must be answered within a certain time, otherwise the mGuard on standby is assigned the “outdated” state and asks the active mGuard for a complete copy of all state information.

The response time is calculated automatically from the fail-over switching time. This is longer than the time for presence notifications (CARP), but shorter than the upper limit of the fail-over switching time.

Loss of presence notifications (CARP) during transmission

A one-off loss of presence notifications (CARP) is tolerated by the mGuard, but it does not tolerate the loss of subsequent presence notifications (CARP). This applies to the availability check on each individual network interface, even when these are checked simultaneously. It is therefore very unlikely that the availability check will fail as a result of a very brief network interruption.

Loss of ICMP echo requests/replies during transmission

ICMP echo requests or replies are important for the connectivity check. Losses are always observed, but are tolerated under certain circumstances.

The following measures can be used to increase the tolerance level on ICMP echo requests.

– Select at least one target must respond under Kind of check in the *Redundancy >> Firewall Redundancy >> Connectivity Checks* menu.
– Also define a secondary set of targets here. The tolerance level for the loss of ICMP echo requests can be further increased by entering the targets of unreliable connections under both sets (primary and secondary) or listing them several times within a set.

Restoring the primary mGuard following a failure

If a redundant pair is defined with different priorities, the secondary mGuard becomes active if the connection fails. The primary mGuard becomes active again after the failure has been rectified. The secondary mGuard receives a presence notification (CARP) and returns to standby mode.

State synchronization

If the primary mGuard becomes active again after a failure of the internal network connection, it may contain an obsolete copy of the firewall database. This database must, therefore, be updated before the connection is reestablished. The primary mGuard ensures that it receives an up-to-date copy before becoming active.

16.1.8 Interaction with other devices

Virtual and actual IP addresses

With firewall redundancy in Router network mode, the mGuard uses actual IP addresses to communicate with other network devices.

Virtual IP addresses are used in the following two cases:

– Virtual IP addresses are used when establishing and operating VPN connections.
– If DNS and NTP services are used according to the configuration, they are offered to internal virtual IP addresses.

The usage of actual (management) IP addresses is especially important for the connectivity check and availability check. Therefore, the actual (management) IP address must be configured so that the mGuard can establish the required connections.

The following are examples of how and why mGuard communication takes place:

– Communication with NTP servers to synchronize the time
– Communication with DNS servers to resolve host names (especially those from VPN partners)
– To register its IP address with a DynDNS service
– To send SNMP traps
– To forward log messages to a SysLog server
– To download a CRL from an HTTP(S) server
– To authenticate a user through a RADIUS server
– To download a configuration profile through an HTTPS server
– To download a firmware update from an HTTPS server

With firewall redundancy in Router network mode, devices connected to the same LAN segment as the redundant pair must use their respective virtual IP addresses as gateways for their routes. If these devices were to use the actual IP address of either of the mGuard devices, this would work until that particular mGuard failed. However, the other mGuard would then not be able to take over.

Targets for the connectivity check

If a target is set for ICMP echo requests as part of the connectivity check, these requests must be answered within a certain time, even if the network is busy with other data. The network path between the redundant pair and these targets must be set so that it is also able to forward the ICMP responses when under heavy load. Otherwise, the connectivity check for an mGuard could erroneously fail.

Targets can be configured for the internal and external interface in the connectivity check (see “Connectivity Checks” on page 313). It is important that these targets are actually connected to the specified interface. An ICMP echo reply cannot be received by an external interface when the target is connected to the internal interface (and vice versa). When the static routes are changed, it is easy to forget to adjust the configuration of the targets accordingly.

The targets for the connectivity check should be well thought out. Without a connectivity check, all it takes are two errors for a network lobotomy to occur.

A network lobotomy is prevented if the targets for both mGuard devices are identical and all targets have to answer the request. However, the disadvantage of this method is that the connectivity check fails more often if one of the targets does not offer high availability.

In **Router network mode**, we recommend defining a highly available device as the target on the external interface. This can be the default gateway for the redundant pair (e.g., a virtual router comprised of two independent devices). In this case, either no targets or a selection of targets should be defined on the internal interface.

Please also note the following information when using a virtual router consisting of two independent devices as the default gateway for a redundant pair. If these devices use VRRP to synchronize their virtual IP, then a network lobotomy could split the virtual IP of this router into two identical copies. These routers could use a dynamic routing protocol and only one may be selected for the data flows of the network being monitored by the mGuard. Only this router should keep the virtual IP. Otherwise, you can define targets which are accessible via this route in the connectivity check. In this case, the virtual IP address of the router would not be a sensible target.

Redundant group

Several redundant pairs can be connected within a LAN segment (redundant group). You define a value as an identifier (through the router ID) for each virtual instance of the redundant pair. As long as these identifiers are different, the redundant pairs do not come into conflict with each other.

Data traffic

In the event of a high **latency** in a network used for state synchronization updates or a serious data loss on this network, the mGuard on standby is assigned the “outdated” state. This does not occur, however, as long as no more than two back-to-back updates are lost. This is because the mGuard on standby automatically requests a repeat of the update. The latency requirements are the same as those detailed under“Fail-over switching time” on page 335.

Sufficient bandwidth

The data traffic generated as a result of the connectivity check, availability check, and state synchronization uses bandwidth on the network. The connectivity check also generates complicated calculations. There are several ways to limit this or stop it completely.

If the influence on other devices is unacceptable:

– The connectivity check must either be deactivated, or must only relate to the actual IP address of the other mGuard.
– The data traffic generated by the availability check and state synchronization must be moved to a separate VLAN.
– Switches must be used which allow separation of the VLANs.

Dedicated interface

The *mGuard centerport* supports a **dedicated interface**. This is a reserved, direct Ethernet interface or a dedicated LAN segment, via which the state synchronization is sent. This separates the load physically from the internal LAN segment.

16.1.9 Transmission capacity with firewall redundancy

These values apply to Router network mode when the data traffic for state synchronization is transmitted without encryption. If the transmission capacity described here is exceeded, in the event of errors the switching time may be longer than that set.

Platform		Transmission capacity with firewall redundancy
mGuard centerport		1500 Mbps, bidirectional[1], not more than 400,000 frames/s
mGuard industrial rs mGuard smart mGuard core mGuard pci mGuard blade mGuard delta EAGLE mGuard	with 533 MHz	150 Mbps[1], bidirectional, not more than 12,750 frames/s
mGuard industrial rs mGuard smart mGuard core mGuard pci mGuard blade mGuard delta EAGLE mGuard	with 266 MHz	62 Mbps, bidirectional[1], not more than 5250 frames/s
mGuard rs4000 mGuard rs4000 3G mGuard smart[2] mGuard core[2] mGuard pci[2] SD mGuard delta[2]		62 Mbps, bidirectional[1], not more than 5250 frames/s

[1] Bidirectional includes traffic in both directions. For example, 1500 Mbps means that 750 Mbps is forwarded in each direction.

Fail-over switching time

The fail-over switching time can be set to 1, 3 or 10 seconds in the event of errors.

The upper limit of 1 second is currently only adhered to by the *mGuard centerport*, even under high load.

16.1.10 Limits of firewall redundancy

- In **Router network mode**, firewall redundancy is only supported with the “static” mode.
- Access to the mGuard via the HTTPS, SNMP, and SSH **management protocols** is only possible with an actual IP address from each mGuard. Access attempts to virtual addresses are rejected.
- The following **features cannot** be used with firewall redundancy.
  - A secondary external Ethernet interface
  - A DHCP server
  - A DHCP relay
  - A SEC-Stick server
  - A user firewall
  - CIFS Integrity Monitoring
- The **redundant pair must have the same configuration**. Take this into account when making the following settings:
  - NAT settings (masquerading, port forwarding, and 1:1 NAT)
  - Flood protection
  - Packet filter (firewall rules, MAC filter, advanced settings)
  - Queues and rules for QoS
- Some network connections may be interrupted following a **network lobotomy**. (See “Restoration in the event of a network lobotomy” on page 338).
- After a fail-over, **semi-unidirectional or complex connections** that were established in the second before the fail-over may be interrupted. (See “Fail-over when establishing complex connections” on page 338 and “Fail-over when establishing semi-unidirectional connections” on page 338.)
- Firewall redundancy does not support the **mGuard pci in Driver mode**.
- State synchronization does not replicate the connection tracking entries for **ICMP echo requests** forwarded by the mGuard. Therefore, ICMP echo replies can be dropped according to the firewall rules if they only reach the mGuard after the fail-over is completed. Please note that ICMP echo replies are not suitable for measuring the fail-over switching time.
- **Masquerading** involves hiding the transmitter behind the first virtual IP address or the first internal IP address. This is different to masquerading on the mGuard without firewall redundancy. When firewall redundancy is not activated, the external or internal IP address hiding the transmitter is specified in a routing table.

16.2 VPN redundancy

VPN redundancy can only be used together with firewall redundancy.

The concept is the same as for firewall redundancy. In order to detect an error in the system environment, the activity is transmitted from the active mGuard to the mGuard on standby.

At any given point in time, at least one mGuard in the redundant pair is operating the VPN connection (except in the event of a network lobotomy).

Basic requirements for VPN redundancy

VPN redundancy does not have any of its own variables. It currently does not have its own menu in the user interface – it is activated together with firewall redundancy instead.

VPN redundancy can only be used if the corresponding license has been purchased and installed on the mGuard.

As VPN connections must be established for VPN redundancy, a corresponding VPN license is also necessary.

If you only have the license for firewall redundancy and VPN connections are installed, VPN redundancy cannot be activated. An error message is displayed as soon as an attempt is made to use firewall redundancy.

Only identical mGuard devices can be used together in a redundant pair.

16.2.1 Components in VPN redundancy

The components used in VPN redundancy are the same as described under firewall redundancy. One additional component is available here – VPN state synchronization. A small number of components are slightly expanded for VPN redundancy. However, the connectivity check, availability check, and firewall state synchronization are all performed in the same way as before.

VPN state synchronization

The mGuard supports the configuration of firewall rules for the VPN connection.

VPN state synchronization monitors the state of the different VPN connections on the active mGuard. It ensures that the mGuard on standby receives a valid, up-to-date copy of the VPN state database.

As with state synchronization of the firewall, VPN state synchronization sends updates from the active mGuard to the mGuard on standby. If requested to do so by the mGuard on standby, the active mGuard sends a complete record of all state information.

Dedicated interface (mGuard centerport)

In the case of the *mGuard centerport*, you can permanently assign the third Ethernet interface for the VPN state synchronization.

As with the state synchronization of the firewall, the data traffic for the VPN state synchronization for the dedicated interface is transmitted when a variable is set. Under *Redundancy >> Firewall Redundancy >> Redundancy* set the *Interface which is used for state synchronization* to **Dedicated Interface**.

Establishing VPN connections

In VPN redundancy, the virtual network interface is used for an additional purpose – to establish, accept, and operate the VPN connections. The mGuard only listens on the first virtual IP address.

In Router network mode, it listens at the first external and internal virtual IP addresses.

State monitoring

State monitoring is used to monitor state synchronization on both the VPN and firewall.

Status indicator

The status indicator shows additional detailed information on the status of VPN state synchronization. This is located directly next to the information for firewall state synchronization.

As an ancillary effect, the status indicator of the VPN connection can also be seen on the mGuard on standby. You can, therefore, find the contents of the VPN state database replicated under the normal status indicator for the VPN connection (under *IPsec VPN >> IPsec Status)*.

Only the state of the synchronization process is shown in the status indicator for firewall redundancy *(Redundancy >> FW Redundancy Status >> Redundancy Status)*.

16.2.2 Interaction of the VPN redundancy components

The individual components interact in the same way as described for firewall redundancy. VPN state synchronization is also controlled by state monitoring. The state is recorded and updates are sent.

Certain conditions must be met for the states to occur. VPN state synchronization is taken into account here.

16.2.3 Error compensation through VPN redundancy

VPN redundancy compensates for the exact same errors as firewall redundancy (see “Error compensation through firewall redundancy” on page 337).

However, the VPN section can hinder the other VPN gateways in the event of a network lobotomy. The independent mGuard devices then have the same virtual IP address for communicating with the VPN partners. This can result in VPN connections being established and disconnected in quick succession.

16.2.4 Setting the variables for VPN redundancy

If the required license keys are installed, VPN redundancy is automatically activated at the same time as firewall redundancy. This occurs as soon as *Enable redundancy* is set to **Yes** in the *Redundancy >> Firewall Redundancy >> Redundancy* menu.

There is no separate menu for VPN redundancy. The existing firewall redundancy variables are expanded.

Table 16-3 Expanded functions with VPN redundancy activated

Redundancy >> Firewall Redundancy >> Redundancy		
General	**Enable redundancy**	Firewall redundancy and VPN redundancy are activated or deactivated.
Virtual interfaces	**External virtual IP addresses**	Only in Router network mode. The mGuard uses the first external virtual IP address as the address from which it sends and receives IKE messages. The external virtual IP address is used instead of the actual primary IP address of the external network interface. The mGuard no longer uses the actual IP address to send or answer IKE messages. ESP data traffic is handled similarly, but is also accepted and processed by the actual IP address.
	Internal virtual IP addresses	As described under *External virtual IP addresses*, but for internal virtual IP addresses.

16.2.5 Requirements for VPN redundancy

– VPN redundancy can only be activated if a **license key** is installed for VPN redundancy and a VPN connection is activated.

– **mGuard rs4000 3G, mGuard rs4000, and mGuard industrial rs only**

  If a VPN connection is controlled via a **VPN switch**, then VPN redundancy cannot be activated.

  (See under: *IPsec VPN* >> *Global* >> *Options* >> *VPN Switch*)

During VPN state synchronization, the state of the VPN connection is sent continuously from the active mGuard to the one on standby so that it always has an up-to-date copy in the event of errors. The only exception is the state of the IPsec replay window. Changes there are only transmitted sporadically.

The volume of the data traffic for state synchronization does not depend on the data traffic sent over the VPN channels. The data volumes for state synchronization are defined by a range of parameters that are assigned to the ISAKMP SAs and IPsec SAs.

16.2.6 Handling VPN redundancy in extreme situations

The conditions listed under “Handling firewall redundancy in extreme situations” on page 338 also apply to VPN redundancy. They also apply when the mGuard is used exclusively for forwarding VPN connections. The mGuard forwards the data flows via the VPN channels and rejects incorrect packets, regardless of whether firewall rules have been defined for the VPN connections or not.

An error interrupts the flow of data traffic

An error that interrupts the data traffic running via the VPN channels represents an extreme situation. In this case, the IPsec data traffic is briefly vulnerable to replay attacks. (A replay attack is the repetition of previously sent encrypted data packets using copies which have been saved by the attacker.) The data traffic is protected by sequential numbers. Independent sequential numbers are used for each direction in an IPsec channel. The mGuard drops ESP packets which have the same sequential number as a packet that has already been decrypted for a specific IPsec channel by the mGuard. This mechanism is known as the **IPsec replay window**.

The IPsec replay window is only replicated sporadically during state synchronization, as it is very resource-intensive. Therefore, the active mGuard may have an obsolete IPsec replay window following a fail-over. An attack is then possible until the real VPN partner has sent the next ESP packet for the corresponding IPsec SA, or until the IPsec SA has been renewed.

To avoid having an insufficient sequential number for the outgoing IPsec SA, VPN redundancy adds a constant value to the sequential number for each outgoing IPsec SA before the mGuard becomes active. This value is calculated so that it corresponds to the maximum number of data packets which can be sent through the VPN channel during the maximum fail-over switching time. In the worst case (1 Gigabit Ethernet and a switching time of 10 seconds), this is 0.5% of an IPsec sequence. At best, this is only one per thousand.

Adding a constant value to the sequential number prevents the accidental reuse of a sequence number already used by the other mGuard shortly before it failed. Another effect is that ESP packets sent from the previously active mGuard are dropped by the VPN partner if new ESP packets are received earlier from the mGuard that is currently active. To do this, the latency on the network must differ from the fail-over switching time.

An error interrupts the initial establishment of the ISAKMP SA or IPsec SA

If an error interrupts the initial establishment of the ISAKMP SA or IPsec SA, the mGuard on standby can continue the process seamlessly, as the state of the SA is replicated synchronously. The response to an IKE message is only sent from the active mGuard after the mGuard on standby has confirmed receipt of the corresponding VPN state synchronization update.

When an mGuard becomes active, it immediately repeats the last IKE message which should have been sent from the previously active mGuard. This compensates for cases where the previously active mGuard has sent the state synchronization but has failed before it could send the corresponding IKE message.

In this way, the establishment of the ISAKMP SA or IPsec SA is only delayed by the switching time during a fail-over.

An error interrupts the renewal of an ISAKMP SA

If an error interrupts the renewal of an ISAKMP SA, this is compensated in the same way as during the initial establishment of the SA. The old ISAKMP SA is also kept for Dead Peer Detection until the renewal of the ISAKMP SA is complete.

An error interrupts the renewal of an IPsec SA

If an error interrupts the renewal of an IPsec SA, this is compensated in the same way as during the initial establishment of the SA. Until renewal of the ISAKMP SA is complete, the old outgoing and incoming IPsec SAs are retained until the VPN partner notices the change.

VPN state synchronization ensures that the old IPsec SAs are retained throughout the entire time that the mGuard remains on standby. When the device becomes active, it can then continue with the encryption and decryption of the data traffic without the need for further action.

Loss of data packets during VPN state synchronization

State synchronization can cope with the loss of one of two back-to-back update packets. If more data packets are lost, this can result in a longer switching time in the event of errors.

The mGuard on standby has an obsolete machine certificate

X.509 certificates and private keys used by a redundant pair to authenticate itself as a VPN partner may need to be changed. The combination of a private key and certificate is hereafter referred to as a machine certificate.

Each mGuard in a redundant pair must be reconfigured in order to switch the machine certificate. Both mGuard devices also require the same certificate so that their VPN partners view them as one and the same virtual VPN device.

As each mGuard has to be reconfigured individually, it may be the case that the mGuard on standby has an obsolete machine certificate for a brief period.

If the mGuard on standby becomes active at the exact moment when the ISAKMP SAs are being established, this procedure cannot be continued with an obsolete machine certificate.

As a countermeasure, VPN state synchronization replicates the machine certificate from the active mGuard to the mGuard on standby. In the event of a fail-over, the mGuard on standby will only use this to complete the process of establishing the ISAKMP SAs where this has already been started.

If the mGuard on standby establishes new ISAKMP SAs after a fail-over, it uses the machine certificate that has already been configured.

VPN state synchronization therefore ensures that the currently used machine certificates are replicated. However, it does not replicate the configuration itself.

The mGuard **on standby has an obsolete Pre-Shared Key (PSK)**

Pre-Shared Keys (PSK) also need to be renewed on occasion in order to authenticate VPN partners. The redundant mGuard devices may then have a different PSK for a brief period. In this case, only one of the mGuard devices can establish a VPN connection as most VPN partners only accept one PSK. The mGuard does not offer any countermeasures for this.

We therefore recommend using X.509 certificates instead of PSKs.

If VPN state synchronization replicates the PSKs being sent to the mGuard on standby for a prolonged period, an incorrect configuration remains concealed during this period, making it difficult to detect.

16.2.7 Interaction with other devices

Resolving host names

If host names are configured as VPN gateways, the mGuard devices in a redundant pair must be able to resolve the host names for the same IP address. This applies especially when *DynDNS Monitoring* (see *Page 253*) is activated.

If the host names are resolved from the mGuard on standby to another IP address, the VPN connection to this host is interrupted following a fail-over. The VPN connection is reestablished through another IP address. This takes place directly after the fail-over. However, a short delay may occur, depending (among other things) on what value is entered under *DynDNS Monitoring* for the *Refresh Interval (sec)*.

Obsolete IPsec replay window

IPsec data traffic is protected against unauthorized access. To this end, each IPsec channel is assigned an independent sequential number. The mGuard drops ESP packets which have the same sequential number as a packet that has already been decrypted for a specific IPsec channel by the mGuard. This mechanism is known as the **IPsec replay window**. It prevents replay attacks, where an attacker sends previously recorded data to simulate someone else's identity.

The IPsec replay window is only replicated sporadically during state synchronization, as it is very resource-intensive. Therefore, the active mGuard may have an obsolete IPsec replay window following a fail-over. This means that a replay attack is possible for a brief period until the real VPN partner has sent the next ESP packet for the corresponding IPsec SA, or until the IPsec SA has been renewed. However, the traffic must be captured completely for this to occur.

Dead Peer Detection

Please note the following point for Dead Peer Detection.

With Dead Peer Detection, set a higher timeout than the upper limit for the *Fail-over switching time* on the redundant pair.

(See under: *IPsec VPN >> Connections >> Edit >> IKE Options, Delay between requests for a sign of life)*

Otherwise, the VPN partners may think that the redundant pair is dead, even though it is only dealing with a fail-over.

Data traffic

In the event of a high latency in a network used for state synchronization updates, the mGuard on standby is assigned the “outdated” state. The same thing also happens in the event of serious data losses on this network.

This does not occur, however, as long as no more than two back-to-back updates are lost. This is because the mGuard on standby automatically requests a repeat of the update. The latency requirements are the same as those detailed under“Fail-over switching time” on page 335.

Actual IP addresses

VPN partners may not send ESP traffic to the actual IP address of the redundant pair. VPN partners must always use the virtual IP address of the redundant pair to send IKE messages or ESP traffic.

16.2.8 Transmission capacity with VPN redundancy

These values apply to Router network mode when the data traffic for state synchronization is transmitted without encryption. If the transmission capacity described here is exceeded, in the event of errors the switching time may be longer than that set.

Platform		Transmission capacity with firewall redundancy
mGuard centerport		220 Mbps bidirectional[1], not more than 60,000 frames/s
mGuard industrial rs mGuard smart mGuard core mGuard pci mGuard blade mGuard delta EAGLE mGuard	with 533 MHz	50 Mbps, bidirectional[1], not more than 5550 frames/s
mGuard industrial rs mGuard smart mGuard core mGuard pci mGuard blade mGuard delta EAGLE mGuard	with 266 MHz	17 Mbps, bidirectional[1], not more than 2300 frames/s
mGuard rs4000 mGuard rs4000 3G mGuard smart[2] mGuard core[2] mGuard pci[2] SD mGuard delta[2]		17 Mbps, bidirectional[1], not more than 2300 frames/s

[1] Bidirectional includes traffic in both directions. For example, 1500 Mbps means that 750 Mbps is forwarded in each direction.

Fail-over switching time

The fail-over switching time can be set to 1, 3 or 10 seconds in the event of errors.

The upper limit of 1 second is currently only adhered to by the mGuard centerport, even under high load.

16.2.9 Limits of VPN redundancy

The limits documented above for firewall redundancy also apply to VPN redundancy (see “Limits of firewall redundancy” on page 344). Further restrictions also apply.

- The redundant pair must **have the same configuration** with respect to the following:
  - General VPN settings
  - Each individual VPN connection
- The mGuard only accepts VPN connections on the **first virtual IP address**.
  - In Router network mode, this means the first internal IP address and the first external IP address.
- The following **features cannot** be used with VPN redundancy:
  - Dynamic activation of the VPN connections using a VPN switch or the CGI script command nph-vpn.cgi (only on mGuard rs4000 3G and mGuard rs4000)
  - Archiving of diagnostic messages for VPN connections
- VPN connections are only supported in Tunnel mode. Transport mode does not take sufficient account of VPN connections.
- The upper limit of the **fail-over switching time** does not apply to connections which are **encapsulated with TCP**. Connections of this type are interrupted for a prolonged period during a fail-over. The encapsulated TCP connections must be reestablished by the initiating side after each fail-over. If the fail-over occurred on the initiating side, they can start immediately after the transfer. However, if the fail-over occurred on the answering side, the initiator must first detect the interruption and then reestablish the connection.
- VPN redundancy supports **masquerading** in the same way as without VPN redundancy. This applies when a redundant pair is masked by a NAT gateway with a dynamic IP address.

  For example, a redundant pair can be hidden behind a DSL router, which masks the redundant pair with an official IP address. This DSL router forwards the IPsec data traffic (IKE and ESP, UDP ports 500 and 4500) to the virtual IP addresses. If the dynamic IP address changes, all active VPN connections which run via the NAT gateway are reestablished.

  The connections are reestablished by means of Dead Peer Detection (DPD) using the relevant configured time. This effect is beyond the influence of the mGuard.
- The redundancy function on the mGuard does not support **path redundancy**. Path redundancy can be achieved using other methods, e.g., by using a router pair. This router pair is seen on the virtual side of the mGuard devices. By contrast, on the other side, each of the routers has different connections.

  Path redundancy must not use NAT mechanisms such as masquerading to hide the virtual IP addresses of the mGuard devices. Otherwise, a migration from one path to another would change the IP addresses used to mask the redundant pair. This would mean that all VPN connections (all ISAKMP SAs and all IPsec SAs) would have to be reestablished.

  The connections are reestablished by means of Dead Peer Detection (DPD) using the relevant configured time. This effect is beyond the influence of the mGuard.
- In the event of path redundancy caused by a network lobotomy, the VPN connections are no longer supported. A network lobotomy must be prevented whenever possible.

X.509 certificates for VPN authentication

The mGuard supports the use of X.509 certificates when establishing VPN connections. This is described in detail under “Authentication” on page 269.

However, there are some special points to note when X.509 certificates are used for authenticating VPN connections in conjunction with firewall redundancy and VPN redundancy.

Switching machine certificates

A redundant pair can be configured so that it uses an X.509 certificate and the corresponding private key together to identify itself to a remote VPN partner as an individual virtual VPN instance.

These X.509 certificates must be renewed regularly. If the VPN partner is set to check the validity period of the certificates, these certificates must be renewed before their validity expires (see “Certificate settings” on page 195).

If a machine certificate is replaced, all VPN connections which use it are restarted by the mGuard. While this is taking place, the mGuard cannot forward any data via the affected VPN connections for a certain period of time. This period depends on the number of VPN connections affected, the performance of the mGuard and VPN partners, and the latency of the mGuard devices on the network.

If this is not feasible for redundancy, the VPN partners of a redundant pair must be configured so that they accept all certificates whose validity is confirmed by a set of specific CA certificates (see “CA Certificates” on page 199 and “Authentication” on page 269).

To do this, select Signed by any trusted CA under *IPsec VPN* >> *Connections* >> *Edit* >> *Authentication* / *Remote CA Certificate.*

If the new machine certificate is issued from a different sub-CA certificate, the VPN partner must be able to recognize this before the redundant pair can use the new machine certificate.

The machine certificate must be replaced on both mGuard devices in a redundant pair. However, this is not always possible if one cannot be reached. This might be the case in the event of a network failure, for example. The mGuard on standby may then have an obsolete machine certificate when it becomes active. This is another reason for setting the VPN partners so that they use both machine certificates.

The machine certificate is normally also replicated with the corresponding key during VPN state synchronization. In the event of a fail-over, the other mGuard can take over and even continue establishing incomplete ISAKMP SAs.

Switching the remote certificates for a VPN connection

The mGuard can be set to authenticate VPN partners directly using the X.509 certificates shown by these VPN partners. For this to happen, the relevant X.509 certificate must be set on the mGuard. This is known as the *Remote CA Certificate*.

If a remote certificate is renewed, for a brief period, only one of the mGuard devices will have a new certificate. We therefore recommend authenticating the VPN partners using CA certificates instead of remote certificates in VPN redundancy.

Adding a new CA certificate to identify VPN partners

The mGuard can be set to authenticate VPN partners using CA certificates (see “CA Certificates” on page 199 and “Authentication” on page 269).

To do this, select Signed by any trusted CA under *IPsec VPN* >> *Connections* >> *Edit* >> *Authentication* / *Remote CA Certificate.*

With this setting, a new CA certificate can be added without affecting the established VPN connections. However, the new CA certificates are used immediately. The X.509 certificate used by the VPN partner to authenticate itself to the mGuard can then be replaced with minimal interruption. The only requirement is ensuring that the new CA certificate is available first.

The mGuard can be set to check the validity period of the certificates provided by the VPN partner (see “Certificate settings” on page 195). In this case, new trusted CA certificates must be added to the mGuard configuration. These certificates should also have a validity period.

If the CRL check is activated (under *Authentication* >> *Certificates* >> *Certificate settings),* one URL (where the corresponding CRL is available) must be maintained for each CA certificate. The URL and CRL must be published before the mGuard uses the CA certificates in order to confirm the validity of the certificates shown by the VPN partners.

Using X.509 certificates with limited validity periods and CRL checks

The use of X.509 certificates is described under “Certificate settings” on page 195 (*“Authentication* >> *Certificates* >> *Certificate settings”* menu).

If X.509 certificates are used and **Check the validity period of certificates and CRLs** is set, the system time has to be correct. We recommend synchronizing the system time using a trusted **NTP server**. Each mGuard in a redundant pair can use the other as an additional NTP server, but not as the only NTP server.

17 Glossary

Asymmetrical encryption

In asymmetrical encryption, data is encrypted with one key and decrypted with a second key. Both keys are suitable for encryption and decryption. One of the keys is kept secret by its owner (private key), while the other is made available to the public (public key), i.e., to potential communication partners.

A message encrypted with the public key can only be decrypted and read by the owner of the associated private key. A message encrypted with the private key can be decrypted by any recipient in possession of the associated public key. Encryption using the private key shows that the message actually originated from the owner of the associated public key. Therefore, the expression “digital signature” is also often used.

However, asymmetrical encryption methods such as RSA are both slow and susceptible to certain types of attack. As a result, they are often combined with some form of symmetrical encryption (→ “Symmetrical encryption” on page 364). On the other hand, concepts are available enabling the complex additional administration of symmetrical keys to be avoided.

DES/3DES

This symmetrical encryption algorithm (→ “Symmetrical encryption” on page 364) was developed by IBM and checked by the NSA. DES was specified in 1977 by the American National Bureau of Standards (the predecessor of the National Institute of Standards and Technology (NIST)) as the standard for American governmental institutions. As this was the very first standardized encryption algorithm, it quickly won acceptance in industrial circles, both inside and outside America.

DES uses a 56-bit key length, which is no longer considered secure as the available processing power of computers has greatly increased since 1977.

3DES is a version of DES. It uses keys that are three times as long, i.e., 168 bits in length. Still considered to be secure today, 3DES is included in the IPsec standard, for example.

AES

AES (Advanced Encryption Standard) has been developed by NIST (National Institute of Standards and Technology) over the course of many years of cooperation with industry. This symmetrical encryption standard has been developed to replace the earlier DES standard. AES specifies three different key lengths (128, 192, and 256 bits).

In 1997, NIST started the AES initiative and published its conditions for the algorithm. From the many proposed encryption algorithms, NIST selected a total of five algorithms for closer examination – MARS, RC6, Rijndael, Serpent, and Twofish. In October 2000, the Rijndael algorithm was adopted as the encryption algorithm.

CA certificate

How trustworthy is a certificate and the issuing CA (certification authority)? (→ “X.509 certificate” on page 363) A CA certificate can be consulted in order to check a certificate bearing this CA's signature. This check only makes sense if there is little doubt that the CA certificate originates from an authentic source (i.e., is authentic). In the event of doubt, the CA certificate itself can be checked. If (as is usually the case) the certificate is a sub-CA certificate (i.e., a CA certificate issued by a sub-certification authority), then the CA certificate of the superordinate CA can be used to check the CA certificate of the subordinate instance. If a superordinate CA certificate is in turn subordinate to another superordinate CA, then its CA certificate can be used to check the CA certificate of the subordinate instance, etc. This “chain of trust” continues down to the root instance (the root CA or certification authority). The root CA's CA file is necessarily self-signed, since this instance is the highest available and is ultimately the basis of trust. No-one else can certify that this instance is actually the instance in question. A root CA therefore is a state or a state-controlled organization.

The mGuard can use its imported CA certificates to check the authenticity of certificates shown by partners. In the case of VPN connections, for example, partners can only be authenticated using CA certificates. This requires all CA certificates to be installed on the mGuard in order to form a chain with the certificate shown by the partner. In addition to the CA certificate from the CA whose signature appears on the certificate shown by the VPN partner to be checked, this also includes the CA certificate of the superordinate CA, and so forth, up to the root certificate. The more meticulously this “chain of trust” is checked in order to authenticate a partner, the higher the level of security will be.

Client/server

In a client/server environment, a server is a program or computer which accepts and responds to queries from client programs or client computers.

In data communication, the computer establishing a connection to a server (or host) is also called a client. In other words, the client is the calling computer and the server (or host) is the computer called.

Datagram

In the IP transmission protocol, data is sent in the form of data packets. These are known as IP datagrams. An IP datagram is structured as follows

IP header	TCP, UDP, ESP, etc. header	Data (payload)

The IP header contains:

– The IP address of the sender (source IP address)
– The IP address of the recipient (destination IP address)
– The protocol number of the protocol on the superordinate protocol layer (according to the OSI layer model)
– The IP header checksum used to check the integrity of the received header

The TCP/UDP header contains the following information:

– The port of the sender (source port)
– The port of the recipient (destination port)
– A checksum covering the TCP header and information from the IP header (e.g., source and destination IP addresses)

Default route

If a computer is connected to a network, the operating system creates a routing table internally. The table lists the IP addresses that the operating system has identified based on the connected computers and the routes available at that time. Accordingly, the routing table contains the possible routes (destinations) for sending IP packets. If IP packets are to be sent, the computer's operating system compares the IP addresses stated in the IP packets with the entries in the routing table in order to determine the correct route.

If a router is connected to the computer and its internal IP address (i.e., the IP address of the router's LAN port) has been relayed to the operating system as the default gateway (in the network card's TCP/IP configuration), then this IP address is used as the destination if all other IP addresses in the routing table are not suitable. In this case, the IP address of the router specifies the default route because all IP packets whose IP address has no counterpart in the routing table (i.e., cannot find a route) are directed to this gateway.

DynDNS provider

Also known as *Dynamic DNS provider*. Every computer connected to the Internet has an IP address (IP = Internet Protocol). If the computer accesses the Internet via a dial-up modem, ISDN or ADSL, its Internet service provider will assign it a dynamic IP address. In other words, the address changes for each online session. Even if a computer is online 24 hours a day without interruption (e.g., flat-rate), the IP address will change during the session.

If this computer needs to be accessible via the Internet, it must have an address that is known to the remote partner. This is the only way to establish a connection to the computer. However, if the address of the computer changes constantly, this will not be possible. This problem can be avoided if the operator of the computer has an account with a DynDNS provider (DNS = Domain Name Server).

In this case, the operator can set a host name with this provider via which the computer should be accessible, e.g., www.example.com. The DynDNS provider also provides a small program that must be installed and run on the computer concerned. Every time a new Internet session is launched on the local computer, this tool sends the IP address used by the computer to the DynDNS provider. The domain name server registers the current assignment of the host name to the IP address and also informs the other domain name servers on the Internet accordingly.

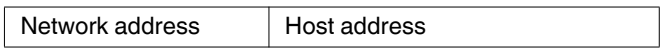
If a remote computer now wishes to establish a connection to a computer that is registered with the DynDNS provider, then the remote computer can use the host name of the computer as the address. This establishes a connection to the responsible DNS in order to look up the IP address that is currently registered for this host name. The corresponding IP address is sent back from the DNS to the remote computer, which can then use it as the destination address. This now leads directly to the desired computer.

In principle, all Internet addresses are based on this procedure: first, a connection to a DNS is established in order to determine the IP address assigned to the host name. Once this has been accomplished, the established IP address is used to set up a connection to the required partner, which could be any site on the Internet.

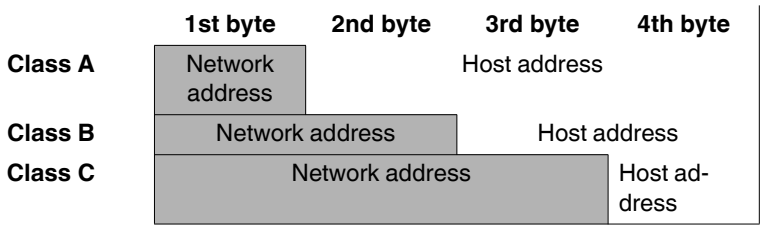
IP address

Every host or router on the Internet/Intranet has its own unique IP address (IP = Internet Protocol). An IP address is 32 bits (4 bytes) long and is written as four numbers (each between 0 and 255), which are separated by a dot.

An IP address consists of two parts: the network address and the host address.



All network hosts have the same network address, but different host addresses. The two parts of the address differ in length depending on the size of the respective network (networks are categorized as Class A, B or C).



The first byte of the IP address determines whether the IP address of a network device belongs to Class A, B or C. The following is specified:

	Value of byte 1	Bytes for the network address	Bytes for the host address
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

Based on the above figures, the number of Class A networks worldwide is limited to 126. Each of these networks can have a maximum of 256 x 256 x 256 hosts (3 bytes of address area). There can be 64 x 256 Class B networks and each of these networks can have up to 65,536 hosts (2 bytes of address area: 256 x 256). There can be 32 x 256 x 256 Class C networks and each of these networks can have up to 256 hosts (1 byte of address area).

Subnet mask

Normally, a company network with access to the Internet is only officially assigned a single IP address, e.g., 123.456.789.21. The first byte of this example address indicates that this company network is a Class B network; in other words, the last two bytes are free to be used for host addressing. Accordingly, an address area for up to 65,536 possible hosts (256 x 256) can be computed.

Such a huge network is not practical and generates a need for subnetworks to be built. The subnet mask is used here. Like an IP address, the mask is 4 bytes long. The bytes representing the network address are each assigned the value 255. The primary purpose of doing this is to enable a portion of the host address area to be “borrowed” and used for addressing subnetworks. For example, if the subnet mask 255.255.255.0 is used on a Class B network (2 bytes for the network address, 2 bytes for the host address), the third byte, which was actually intended for host addressing, can now be used for subnetwork addressing. This computes to potential support for 256 subnetworks, each with 256 hosts.

IPsec

IP security (IPsec) is a standard that uses encryption to verify the authenticity of the sender and to ensure the confidentiality and integrity of the data in IP datagrams (→ “Datagram” on page 358). The components of IPsec are the Authentication Header (AH), the Encapsulating Security Payload (ESP), the Security Association (SA), and the Internet Key Exchange (IKE).

At the start of the session, the systems involved in communication must determine which technique should be used and the implications of this choice, e.g., *Transport Mode* or *Tunnel Mode*.

In *Transport Mode*, an IPsec header is inserted between the IP header and the TCP or UDP header respectively in each IP datagram. Since the IP header remains unchanged, this mode is only suitable for host-to-host connections.

In *Tunnel mode*, an IPsec header and a new IP header are prefixed to the entire IP datagram. This means the original datagram is encrypted in its entirety and stored in the payload of the new datagram.

Tunnel Mode is used in VPN applications: the devices at the ends of the tunnel ensure that the datagrams are encrypted/decrypted; in other words, the actual datagrams are completely protected during transfer over a public network.

Subject, certificate

In a certificate, confirmation is provided by a certification authority (CA) that the certificate does actually belong to its owner. This is done by confirming specific owner properties. Furthermore, the certificate owner must possess the private key that matches the public key in

the certificate. (→ “X.509 certificate” on page 363).

Example

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
    Validity
      Not Before: Oct 29 17:39:10 2000 GMT
→ Subject: CN=anywhere.com,E=doctrans.de,C=DE,ST=Hamburg,L=Hamburg,O=Innominate,OU=Security
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
          d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
          9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
          90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
          1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
          7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
          50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
          8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
          f0:b4:95:f5:f9:34:9f:f8:43
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Alternative Name:
        email:xyz@anywhere.com
      Netscape Comment:
        mod_ssl generated test server certificate
      Netscape Cert Type:
        SSL Server
  Signature Algorithm: md5WithRSAEncryption
    12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
    3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
    82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
    cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
    4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
    d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
    44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
    ff:8e
```

The *subject distinguished name* (or *subject* for short) uniquely identifies the certificate owner. The entry consists of several components. These are known as attributes (see the example certificate above). The following table contains a list of possible attributes. The sequence of attributes in an X.509 certificate can vary.

Table 17-1 X.509 Certificate

Abbreviation	Name	Explanation
CN	Common name	Identifies the person or object to whom or which the certificate belongs. Example: CN=server1
E	E-mail address	Specifies the e-mail address of the certificate owner.
OU	Organizational unit	Specifies the department within an organization or company. Example: O=Development
O	Organization	Specifies the organization or company. Example: O=Innominate

Table 17-1 X.509 Certificate

Abbreviation	Name	Explanation
L	Locality	Specifies the place/locality. Example: L=Hamburg
ST	State	Specifies the state or county. Example: ST=Bavaria
C	Country	Two-letter code that specifies the country. (Germany=DE) Example: C=DE

A filter can be set for the subject (i.e., the certificate owner) during VPN connections and remote service access to the mGuard using SSH or HTTPS. This would ensure that only certificates from partners are accepted that have certain attributes in the subject line.

NAT (Network Address Translation)

Network Address Translation (NAT) (also known as *IP masquerading*) "hides" an entire network behind a single device, known as a NAT router. If you communicate externally via a NAT router, the internal computers in the local network and their IP addresses remain hidden. The remote communication partner will only see the NAT router with its IP address.

In order to allow internal computers to communicate directly with external computers (on the Internet), the NAT router must modify the IP datagrams that are sent from internal computers to remote partners and received by internal computers from remote partners.

If an IP datagram is sent from the internal network to a remote partner, the NAT router modifies the UDP and TCP headers of the datagram, replacing the source IP address and source port with its own official IP address and a previously unused port. For this purpose, the NAT router uses a table in which the original values are listed together with the corresponding new ones.

When a response datagram is received, the NAT router uses the specified destination port to recognize that the datagram is intended for an internal computer. Using the table, the NAT router replaces the destination IP address and port before forwarding the datagram via the internal network.

Port number

A port number is assigned to each device in UDP and TCP protocol-based communication. This number makes it possible to differentiate between multiple UDP or TCP connections between two computers and use them simultaneously.

Certain port numbers are reserved for specific purposes. For example, HTTP connections are usually assigned to TCP port 80 and POP3 connections to TCP port 110.

Proxy

A proxy is an intermediary service. A web proxy (e.g., Squid) is often connected upstream of a large network. For example, if 100 employees access a certain website frequently over a web proxy, then the proxy only loads the relevant web pages from the server once and then distributes them as needed among the employees. Remote web traffic is reduced, which saves money.

PPPoE

Acronym for **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. A protocol based on the PPP and Ethernet standards. PPPoE is a specification defining how to connect users to the Internet via Ethernet using a shared broadband medium such as DSL, wireless LAN or a cable modem.

PPTP

Acronym for **P**oint-to-**P**oint **T**unneling **P**rotocol. This protocol was developed by Microsoft and U.S. Robotics, among others, for secure data transfer between two VPN nodes (→ VPN) via a public network.

Router

A router is a device that is connected to different IP networks and communicates between them. To do this, the router has an interface for each network connected to it. A router must find the correct path to the destination for incoming data and define the appropriate interface for forwarding it. To do this, it takes data from a local routing table listing assignments between available networks and router connections (or intermediate stations).

Trap

SNMP (Simple Network Management Protocol) is often used alongside other protocols, in particular on large networks. This UDP-based protocol is used for central administration of network devices. For example, the configuration of a device can be requested using the GET command and changed using the SET command; the requested network device must simply be SNMP-compatible.

An SNMP-compatible device can also send SNMP messages (e.g., should unexpected events occur). Messages of this type are known as SNMP traps.

X.509 certificate

A type of “seal” that certifies the authenticity of a public key (→ asymmetrical encryption) and the associated data.

It is possible to use certification to enable the user of the public key (used to encrypt the data) to ensure that the received public key is indeed from its actual issuer (and thus from the instance that should later receive the data). A *certification authority* (CA) certifies the authenticity of the public key and the associated link between the identity of the issuer and its key. The certification authority verifies authenticity in accordance with its rules (for example, it may require the issuer of the public key to appear before it in person). After successful authentication, the CA adds its (digital) signature to the issuer's public key. This results in a certificate.

An X.509(v3) certificate thus consists of a public key, information about the key owner (the Distinguished Name (DN)), authorized use, etc., and the signature of the CA (→ Subject, certificate).

The signature is created as follows: the CA creates an individual bitstring from the bit string of the public key, owner information, and other data. This bitstring can be up to 160 bits in length and is known as the HASH value. The CA then encrypts this with its own private key and then adds it to the certificate. The encryption with the CA's private key proves the authenticity of the certificate (i.e., the encrypted HASH string is the CA's digital signature). If the certificate data is tampered with, then this HASH value will no longer be correct and the certificate will be rendered worthless.

The HASH value is also known as the fingerprint. Since it is encrypted with the CA's private key, anyone who has the corresponding public key can decrypt the bitstring and thus verify the authenticity of the fingerprint or signature.

The involvement of a certification authority means that it is not necessary for key owners to know each other. They only need to know the certification authority involved in the process. The additional key information also simplifies administration of the key.

X.509 certificates can, for example, be used for e-mail encryption by means of S/MIME or IPsec.

Protocol, transmission protocol

Devices that communicate with each other must follow the same rules. They have to “speak the same language”. Rules and standards of this kind are called protocols or transmission protocols. Some of the more frequently used protocols are IP, TCP, PPP, HTTP, and SMTP.

Service provider

Service providers are companies or institutions that enable users to access the Internet or online services.

Spoofing, anti-spoofing

In Internet terminology, spoofing means supplying a false address. Using this false Internet address, a user can create the illusion of being an authorized user.

Anti-spoofing is the term for mechanisms that detect or prevent spoofing.

Symmetrical encryption

In symmetrical encryption, the same key is used to encrypt and decrypt data. Two examples of symmetrical encryption algorithms are DES and AES. They are fast, but also increasingly difficult to administrate as the number of users increases.

TCP/IP (Transmission Control Protocol/Internet Protocol)

These are network protocols used to connect two computers on the Internet:

IP is the base protocol.

UDP is based on IP and sends individual packets. The packets may reach the recipient in a different order than that in which they were sent or they may even be lost.

TCP is used for connection security and ensures, for example, that data packets are forwarded to the application in the correct order.

UDP and TCP add port numbers between 1 and 65535 to the IP addresses. These distinguish the various services offered by the protocols.

A number of additional protocols are based on UDP and TCP. These include HTTP (Hyper Text Transfer Protocol), HTTPS (Secure Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3), and DNS (Domain Name Service).

ICMP is based on IP and contains control messages.

SMTP is an e-mail protocol based on TCP.

IKE is an IPsec protocol based on UDP.

ESP is an IPsec protocol based on IP.

On a Windows PC, the WINSOCK.DLL (or WSOCK32.DLL) provides a common interface for both protocols.

(→ “Datagram” on page 358)

VLAN

A VLAN (Virtual Local Area Network) divides a physical network into several independent logical networks, which exist in parallel.

Devices on different VLANs can only access devices within their own VLAN. Accordingly, assignment to a VLAN is no longer defined by the network topology alone, but also by the configured VLAN ID.

VLAN settings can be used as optional settings for each IP. A VLAN is identified by its VLAN ID (1 - 4094). All devices with the same VLAN ID belong to the same VLAN and can, therefore, communicate with each other.

The Ethernet packet for a VLAN (according to IEEE 802.1Q) is extended by 4 bytes, with 12 bits available for recording the VLAN ID. VLAN IDs “0” and “4095” are reserved and cannot be used for VLAN identification.

VPN (Virtual Private Network)

A **V**irtual **P**rivate **N**etwork (VPN) connects several separate private networks (subnetworks) via a public network (e.g., the Internet) to form a single common network. A cryptographic protocol is used to ensure confidentiality and authenticity. A VPN is therefore an inexpensive alternative to using permanent lines for building a nationwide company network.